PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059864
(43)Date of publication of application : 25.02.2000

(51)Int.Cl. H04Q 7/38
H04B 7/15
H04B 7/26
H04M 15/00

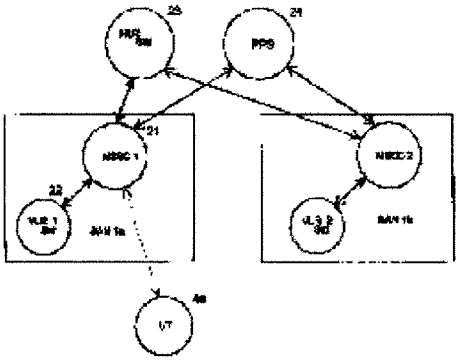
(21)Application number : 11-133303
(22)Date of filing : 13.05.1999

(71)Applicant : ICO SERVICES LTD
(72)Inventor : HUI KELLY

(30)Priority
Priority number : 98 98305186 Priority date : 30.06.1998 Priority country : EP

(54) PREPAID LONG DISTANCE COMMUNICATION METHOD AND DEVICE THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To attain improvement of security by deciding a time and a period of time during which a subscriber is permitted to use services on the basis of the amount of available credit.
SOLUTION: A prepaid server (PPS) 24 identifies a subscriber on the basis of international mobile subscriber's identity(IMSI) information, retrieves a corresponding credit record, uses a destination network identity, dial number information and current time information, and decides a charge table applied to a call. The PPS 24 calculates a call period of time permitted to a specific call generated onto a network. This information is transmitted to a user terminal(UT) and a subscriber's identification module (SIM) by way of a home network MSSC 21 in a standard GSM unstructured supplementary service data(USSD) message. The SIM enables a call on a destination network 8 and instructs the UT to return to normal display. When the connection is established, the SIM activates an internal timer.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－59864
（P2000－59864A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｈ	
Ｈ０４Ｂ　7/15		Ｈ０４Ｍ　15/00	Ｇ	
7/26			Ｚ	
Ｈ０４Ｍ　15/00		Ｈ０４Ｂ　7/15	Ｚ	
		7/26	Ｚ	

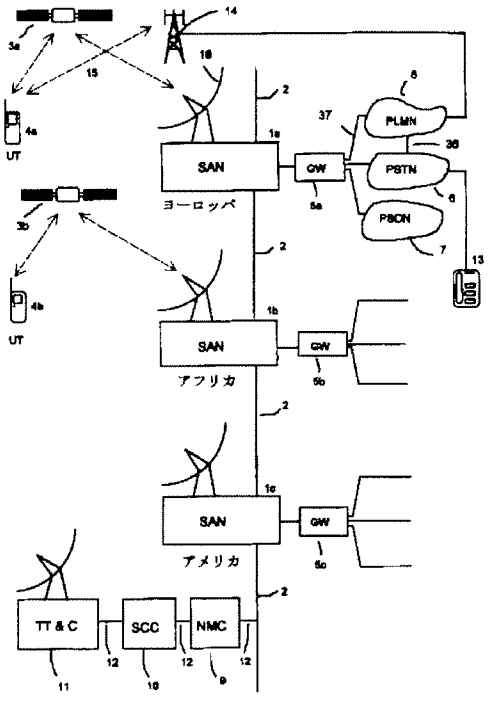
審査請求　未請求　請求項の数16　ＯＬ　（全 13 頁）

(21)出願番号　特願平11－133303
(22)出願日　平成11年５月13日(1999.5.13)
(31)優先権主張番号　９８３０５１８６．３
(32)優先日　平成10年６月30日(1998.6.30)
(33)優先権主張国　ヨーロッパ特許庁（ＥＰ）

(71)出願人　597129263
アイシーオー・サーヴィシーズ・リミテッド
イギリス・Ｗ６・９ＢＮ・ロンドン・クイーン・キャロライン・ストリート・１
(72)発明者　ケリー・ヒュイ
イギリス・Ｗ６・９ＢＮ・ロンドン・クイーン・キャロライン・ストリート・１・シー／オー・アイシーオー・サーヴィシーズ・リミテッド
(74)代理人　100064908
弁理士　志賀　正武　（外９名）

(54)【発明の名称】　料金前払遠距離通信方法および装置

(57)【要約】
【課題】　加入者のクレジット情報を使用者端末へ送信する必要が無く、その結果、保安性に優れた料金前払遠距離通信方法および装置を提供すること。
【解決手段】　衛星移動電話システムへの料金前払加入者は、移動先地上ネットワーク上で、他の全ての加入者と同じサービスを提供される。加入者ネットワークは、各料金前払加入者に対するクレジット記録を保持し、かつ、加入者の利用可能なクレジットが（他のネットワーク上で）許可する呼時間の最大量を（他のネットワーク上のサービスにアクセスすることを求める加入者の使用者端末からの要求に応答して）計算することができる。利用可能な呼時間は、使用者端末へ送信される。該使用者端末は、経過していない呼時間を第１ネットワークへ通知するだけでなく、呼を制御する。



1

【特許請求の範囲】

【請求項１】　第１通信ネットワークへの料金前払加入者が第２通信ネットワークへ移動するときに、該加入者に対して、第２通信ネットワークによって提供される通信サービスへのアクセスを提供する方法であって、
加入者は、該サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、
サービスを使用することを加入者が許可される時間期間を、利用可能なクレジット量に基づいて決定し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする方法。

【請求項２】　請求項１記載の方法において、
加入者が第２ネットワークへ移動している間に、第１ネットワークで時間期間を決定することを具備することを特徴とする方法。

【請求項３】　請求項２記載の方法において、
第１ネットワークに接続された計算手段で時間期間を決定することを具備することを特徴とする方法。

【請求項４】　請求項２記載の方法において、
加入者は、使用者端末を介して、サービスにアクセスでき、
サービスへのアクセスに対する使用者端末からの要求に応じて時間期間を決定することを具備することを特徴とする方法。

【請求項５】　請求項３記載の方法において、
加入者がサービスにアクセスしている使用者端末へ、計算手段から、予め決定された時間期間の送信を開始することを更に具備することを特徴とする方法。

【請求項６】　請求項４記載の方法において、
専有の信号フォーマットを使用した使用者端末への送信のために、予め決定された時間期間を符号化することを具備することを特徴とする方法。

【請求項７】　請求項１記載の方法において、
第１ネットワークは、衛星遠距離通信ネットワークを具備し、かつ、第２ネットワークは、地上ベースの移動ネットワークを具備することを特徴とする方法。

【請求項８】　第１通信ネットワークへの料金前払加入者が第２通信ネットワークへ移動している間に、該加入者に対して、第２通信ネットワークによって提供される通信サービスへの使用者端末を介したアクセスを提供する方法であって、
加入者は、該サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、
加入者によって利用可能なクレジットの量に対応するサービスを使用することを加入者が許可される時間期間の決定を要求する送信を、使用者端末から第１ネットワークへ開始し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする方法。

2

【請求項９】　請求項８記載の方法において、
時間期間決定要求が生成されることを可能とするために、使用者端末によって生成される呼を禁止することを具備することを特徴とする方法。

【請求項１０】　請求項８記載の方法において、
予め決定された時間期間の通知を受信することを具備することを特徴とする方法。

【請求項１１】　請求項８記載の方法において、
現在起こっている呼の期間を予め決定された時間期間と比較することを具備することを特徴とする方法。

【請求項１２】　請求項１０記載の方法において、
予め決定された時間期間が終了すると、サービスを使用して使用者端末によって生成された呼を終了することを具備することを特徴とする方法。

【請求項１３】　請求項８記載の方法において、
サービスを使用して使用者端末によって生成された呼が終了された後、時間期間の送信を第１ネットワークへ開始することを具備することを特徴とする方法。

【請求項１４】　第１ネットワークと第２ネットワークとを具備する遠距離通信ネットワーク構成であって、
該ネットワーク構成は、第１ネットワークへの料金前払加入者が第２ネットワークへ移動するときに、該加入者に対して、第２ネットワーク上の通信サービスへのアクセスを提供し、
加入者は、前記サービス上での使用に対して利用可能な予め決定されたクレジット量を有し、
サービスを使用することを加入者が許可される時間期間を、利用可能なクレジット量に基づいて決定するためのプロセッサを更に具備し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする遠距離通信ネットワーク構成。

【請求項１５】　請求項１４記載のネットワーク構成において、
プロセッサは、第１ネットワークに接続された料金前払サーバーを具備することを特徴とするネットワーク構成。

【請求項１６】　第１通信ネットワークへの料金前払加入者が第２通信ネットワークへ移動するときに、該加入者に対して、第２通信ネットワーク上の通信サービスへの使用者端末を介したアクセスを提供する装置であって、
加入者は、前記サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、
サービスを使用することを加入者が許可される時間期間を、クレジット量に基づいて決定するために、使用者端末からの要求に応答するプロセッサを具備し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、移動遠距離通信ネットワークにおける料金前払遠距離通信サービスの設備に関する。この発明は、特に、自身のホームネットワークから離れて移動している料金前払加入者へ料金前払遠距離通信サービスを提供することに関するが、このことのみに関するわけではない。

【０００２】

【従来の技術および発明が解決しようとする課題】地上移動遠距離通信システムはよく知られており、かつ、（異なる規格に従って動作する）多数の異なるシステムが開発されている。これらの公衆地上移動ネットワーク（ＰＬＭＮ）は、アナログ規格またはデジタル規格に従って動作する。ヨーロッパとほとんどの極東と他の地域とでは、グローバルシステムモバイル（Global System Mobile：ＧＳＭ）ネットワークが普及している。一方、合衆国では、アドバンスドモバイルフォンサービス（Advanced Mobile Phone Service：ＡＭＰＳ）およびディジタルアドバンスドモバイルフォンシステム（DigitalAdvanced Mobile Phone System：ＤＡＭＰＳ）が使われており、かつ、日本では、パーソナルハンディフォンシステム（Personal Handiphone System：ＰＨＳ）およびパーソナルディジタルコミュニケーション（Personal Digital Communication：ＰＤＣ）ネットワークが使用されている。より最近では、世界的な移動遠距離通信システム（ＵＭＴＳ）についての提案がなされている。これらのネットワークは、全て、（移動使用者端末と通信する）送信機／受信機を伴うセルラーネットワークおよび地上ベースのネットワークである。

【０００３】例えば、ＧＳＭシステムに基づくＰＬＭＮでは、ＰＬＭＮの個々のセルは、地理的に間隔をあけられた一連の地上基地トランシーバー局（ＢＴＳ）によって処理されている。ＢＴＳは、基地局コントローラ（ＢＳＣ）を通して、移動スイッチングセンター（ＭＳＣ）へ結合されている。ＭＳＣは、ネットワークから従来の公衆交換電話ネットワーク（ＰＳＴＮ）へのゲートウエーを提供する。ＰＬＭＮは、ホームロケーションレジスタ（ＨＬＲ）を具備する。ＨＬＲは、システムへの加入者と該加入者の使用者端末とに関する情報を記憶する。一般的に、ＧＳＭの顧客は、単一のＰＬＭＮ（ここでは、「加入者のホームネットワーク」として参照する）との契約関係を有する。使用者端末がスイッチを入れられると、該使用者端末はホームネットワークのＨＬＲに自己を登録する。もし、使用者が別のＧＳＭネットワークへ移動すると、使用者端末は、訪問先ネットワークのビジターロケーションレジスタ（ＶＬＲ）に自己を登録する。訪問先ネットワークは、認証および経路指定および他の目的のために、ホームネットワークのＨＬＲと通信する。ＤＡＭＰＳネットワークおよびＰＨＳネットワークおよびＰＤＣネットワークは、類似のロケーションレジスタを有する。

【０００４】より最近では、移動使用者端末と従来の地上ネットワークとの間における衛星通信リンクを使用する多数の異なる移動遠距離通信システムが提案されている。

【０００５】あるネットワークは、いわゆる低地球軌道（ＬＥＯ）衛星の一群を使用する。該低地球軌道衛星は、７８０ｋｍの軌道半径を有する。該ネットワークは、イリジウム（登録商標）衛星セルラーシステムとして知られ、かつ、例えば、欧州特許公開第０３６５８８５号公報および米国特許第５３９４５６１号公報（モトローラ）に記載されている。電話送受器のような移動使用者端末は、頭上の軌道周回衛星へのリンクを確立する。呼は、該軌道周回衛星から、（衛星群内の）他の衛星へ、そして、一般的には（従来の地上ベースのネットワークへ接続されている）地上局へ、送信されることができる。

【０００６】他の案が提案されている。該案は、いわゆる中間地球軌道（ＭＥＯ）衛星群を使用する。該中間地球軌道衛星は、１００００～２００００ｋｍの範囲の軌道半径を伴う。Walker J.G. による”Satellite Patterns for Continuous MultipleWhole Earth Coverage”（1997年、Royal Aircraft Establishment）の第１１９～１２２頁目を参照されたい。さらに、例えば、英国特許公開第２２９５２９６号公報に記載されているＩＣＯ（登録商標）衛星セルラーシステムと、欧州特許公開第０５１０７８９号公報に記載されているオデッセイ（登録商標）衛星セルラーシステムとを参照されたい。これらのシステムでは、衛星通信リンクは、隣接する衛星間における通信を許可しない。代わりに、（移動送受器のような）移動使用者端末からの信号は、最初に衛星へ送信され、そして、地上局（即ち、衛星アクセスノード：ＳＡＮ）へ送信される。ＳＡＮは、従来の地上ベースの電話ネットワークへ接続されている。このことは、「システムの多くの構成要素は（ＧＳＭのような）既知のディジタル地上セルラーテクノロジーと互換性がある」という利点を有する。また、ＬＥＯネットワークを伴う場合よりもより簡単な衛星通信技術が使用されることができる。

【０００７】衛星通信ネットワークでは、軌道周回衛星と通信するために、地上局が、世界中の色々な場所に配置されている。ＩＣＯ（登録商標）システムおよび他のシステムでは、ビジターロケーションレジスタが、各々の衛星地上局と関連付けられている。該衛星地上局は（個々の地上局を使用している）個々の使用者端末の記録を保持する。

【０００８】世界のあるエリアでは、従来の地上ＰＬＭＮによって提供される受信可能範囲と衛星ネットワークによって提供される受信可能範囲とが重なることがあ

る。「個々の使用者端末が地上ＰＬＭＮまたは衛星ネットワークのいずれかを伴って選択的に動作する」ということが提案されている。使用者端末は、使用者がネットワークを選択することを許可するためのスイッチを具備してもよく、他には、（例えば、定義された顧客の選択または他の要因に基づいて）自動的選択が行われてもよい。故に、例えば、ＩＣＯ加入者は、（加入者への課金のために）課金情報および他の待遇情報がＩＣＯシステムへ送り戻されながら、ＰＬＭＮを移動先ネットワークとして使用できる。「通常、費用および信号強度を含む理由のために、（例えば、市街地において）利用可能の時は、従来の地上ＰＬＭＮが好まれる」ということが予見される。

【０００９】他のネットワークへ移動した加入者によるネットワークの使用は、関係するネットワークオペレータ間の移動契約によって管理される。これらの契約は、一般的に、料金表情報の包括的な交換について準備する。それによって、各ネットワークは、移動加入者によって負われるであろう費用を前もって計算できる。例えば、移動契約は、「移動先ネットワークＢが、（特定の位置へ電話をかけている）ホームネットワークＡの加入者に対して、特定の料金表で、（例えば、移動先ネットワークＢが該移動先ネットワークＢの加入者に請求する額に１５％をプラスした額に等しい）移動レートで請求する」ということを提供する。

【００１０】ネットワークＡの加入者がネットワークＢへ移動すると、ネットワークＢは、初めに、ネットワークＡを用いて加入者を認証することを要求する。もし、ネットワークＡが必要な認証を提供するならば、加入者は、ネットワークＢを使用して電話をかけることを許可される。このことは、適切な比率で、該呼に料金請求する。そして、該呼に対する請求書が（一般的に、予め決定された期間に渡ってネットワークＡの全ての加入者へネットワークＢによって提供されたサービスに対して総計された料金の一部として）加入者のホームネットワークＡへ送られる。そして、ホームネットワークＡのオペレータは、ホームネットワークＡの加入者それぞれに課金することができる。ＧＳＭシステムでは、例えば、該料金請求手続は、（各呼に対して生成され、かつ、使用料チケットとして知られる）個々の記録または呼詳細記録に基づく。この原理は、呼を送る際に多数のネットワークが関係する場合に速やかに拡張する。

【００１１】通常の経過時間に基づいて（呼に対して）料金請求するだけでなく、多くのオペレータは、該オペレータ自身の加入者に対して料金前払サービスを提供している。該サービスでは、加入者は、指定された量の呼時間に対して、前もって支払いを行う。多くの加入者にとって、呼費用を制御することを補助するという魅力ある選択であるだけでなく、料金前払サービスは、衛星電話システムのオペレータに対する特に重要な料金請求の形式である。該オペレータにとって、料金前払システムは、該サービスがカバーする多くの国（特に、現金ベースの経済を有する国、または、適切なクレジット照合設備のない国）において支払いを補償する唯一の方法である。

【００１２】しかしながら、料金前払加入者に移動可能性を提供することに関連して、重大な困難が存在する。実例としては、訪問先ネットワークＢがネットワークＡの移動料金前払加入者の内の１人を認証しようとする場合、もし「加入者が該加入者に割り当てられたクレジットを越えて使用しない」ということを保証する方法が何もないならば、ネットワークＡはそのような認証を提供しない。実際には、このことは、呼時間に対する支払いが一度失効すると、加入者の呼をリアルタイムで終了するいくつかの手段を要求する。

【００１３】ＧＳＭネットワークに関して、この問題を解決する１つの可能な方法は、標準ＧＳＭアドバイスオブチャージ（advice of charge：ＡｏＣ）サービスを使用することである。該サービスでは、料金請求情報が、訪問先ネットワークＢから移動使用者端末へ、（移動契約において指定される）料金表契約に基づいて送られる。例えば、呼のセットアップ時に、訪問先ネットワークＢは、適用されるべき料金表を決定するために、料金分析機能を実行する。この料金表は、呼の開始時に、料金請求アドバイス情報（charge advice information：ＣＡＩ）構成要素の形式で、使用者端末へ送信される。該形式は、料金表を、単位料金や単位長等の点で記載している。ＣＡＩの受信時には、使用者端末は、実際の呼料金を計算し、かつ、該呼料金を、使用者端末内の加入者識別モジュール（ＳＩＭ）に記憶された計数値から減算する。ＳＩＭは、利用可能なクレジット情報も記憶している。故に、使用者端末は「利用可能なクレジットが越えられない」ということを保証できる。

【００１４】このアプローチの１つの欠点は、「料金請求情報が電波送信媒体上を使用者端末へ標準ＡＯＣフォーマットで周期的に送信される」ということである。このことは、使用者端末／ＳＩＭインターフェースにおける（無料電話をかけるための）改竄の危険性を助長する。

【００１５】他の欠点は、「もし、呼が多数のネットワーク上を移動料金前払加入者から経路決定されるべきならば、各ネットワークは、ホスト役のネットワークが正確なリアルタイム料金請求情報を移動加入者に提供できるように、ホスト役のネットワーク自身の移動料金表に基づいて、ホスト役のネットワークに、リアルタイムの料金請求情報を提供しなくてはならない」ということである。このことは、標準移動契約に渡りかつ該標準移動契約上において、関連する全てのネットワークオペレータの間における複数の相互的な契約を要求する。さらに、（このことによって生じる）潜在的な国際的ネット

ワーク上でのリアルタイム信号送信における実質的な増加は、「料金前払加入者へ移動能力を提供するという問題に対して、ＡｏＣアプローチが実際には実用的な解決でない」ということを意味する。

【００１６】（リアルタイム料金請求情報が電波送信媒体インターフェース上を送信される）料金前払システムは、R.Krayem-Nevoux, G.Mazziotto, P.Hiolleによる”Payhone Service for Third Generation Mobile Systems”（1993年 IEEE, XP-002088065）に開示されている。この文献は、「ＰＬＭＮと使用者端末との間において電波送信媒体インターフェースを介して送信される構成要素に関する料金請求情報は、変造事実を両者（ＰＬＭＮおよび使用者端末）に知られることなしに変造されることができない」ということを保証するために必要な保安特徴を記載する。

【００１７】本発明は、上記欠点を除去する事を目的とする。

【００１８】

【課題を解決するための手段】本発明によると、第１通信ネットワークへの料金前払加入者が第２通信ネットワークへ移動するときに、該加入者に対して、第２通信ネットワークによって提供される通信サービスへのアクセスを提供する方法であって、加入者は、該サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、サービスを使用することを加入者が許可される時間期間を、利用可能なクレジット量に基づいて決定し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする方法が提供される。

【００１９】本発明による方法は、加入者が第２ネットワークへ移動している間に、第１ネットワークで時間期間を決定することを具備してもよく、このことは、第１ネットワークに接続された計算手段で時間期間を決定することを具備する。

【００２０】本発明の更なる特徴によると、第１通信ネットワークへの料金前払加入者が第２通信ネットワークへ移動している間に、該加入者に対して、第２通信ネットワークによって提供される通信サービスへの使用者端末を介したアクセスを提供する方法であって、加入者は、該サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、加入者によって利用可能なクレジットの量に対応するサービスを使用することを加入者が許可される時間期間の通知を要求する送信を、使用者端末から第１ネットワークへ開始し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする方法が提供される。

【００２１】本発明によると、第１ネットワークと第２ネットワークとを具備する遠距離通信ネットワーク構成であって、該ネットワーク構成は、第１ネットワークへの料金前払加入者が第２ネットワークへ移動するときに、該加入者に対して、第２ネットワーク上の通信サービスへのアクセスを提供し、加入者は、前記サービス上での使用に対して利用可能な予め決定されたクレジット量を有し、サービスを使用することを加入者が許可される時間期間を、利用可能なクレジット量に基づいて決定するためのプロセッサを更に具備し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする遠距離通信ネットワーク構成もまた提供される。

【００２２】本発明によると、第１通信ネットワークへの料金前払加入者が第２通信ネットワークへ移動するときに、該加入者に対して、第２通信ネットワーク上の通信サービスへの使用者端末を介したアクセスを提供する装置であって、加入者は、前記サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、サービスを使用することを加入者が許可される時間期間を、クレジット量に基づいて決定するために、使用者端末からの要求に応答するプロセッサを具備し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする装置が更に提供される。

【００２３】本発明の実施形態から得られる利点は、「ホームネットワークが、移動先ネットワークにとって明白な方法で、呼に対する制御を保持でき、故に、このことは、ネットワークオペレータ間における相互的な契約に対する必要を除去する」ということである。この場合、移動先ネットワークは「処理されている加入者が料金前払加入者である」ということを知らず、そのため、呼の費用とクレジット情報とは、使用者端末へ送信される必要がない。このことは、ネットワークと加入者の保安を強化する。特に、加入者のクレジット情報は、ホームネットワークの単独制御下で保持でき、かつ、たとえ、クレジット情報に対応する呼時間情報が、使用者端末へおよび使用者端末から（本発明の実施形態に従って）送信されるとしても、この送信は、ホームネットワークに専有されるフォーマットで行われ、さらに追加の保安を提供する。

【００２４】

【発明の実施の形態】本発明の実施形態が、一例として、添付図面を参照して、ここで説明される。添付図面は以下の通りである。図１は、本発明による衛星遠距離通信システムの概要図である。該衛星遠距離通信システムは、局所的な地上ベースの移動遠距離通信システムを伴う。図２は、ＳＡＮ１ａの付近における衛星ネットワークおよび関連する地上セルラーネットワークのより詳細なブロック図である。図３は、衛星ネットワーク内の料金前払サーバーの設備を図解する概要ブロック図である。図４は、移動使用者端末の概要図である。図５は、図４に示される使用者端末の回路の概要ブロック図であ

る。図６は、図４および図５に示されるＳＩＭカードの概要ブロック図である。図７は、本発明によるクレジット照合手続を示すフローチャートである。

【００２５】図１を参照すると、衛星移動電話システムは、複数の衛星アクセスノード（ＳＡＮ）１ａ，１ｂ，１ｃと、複数の衛星３ａ，３ｂと、複数の使用者端末（ＵＴ）４ａ，４ｂと、ゲートウエー（ＧＷ）５ａ，５ｂ，５ｃと、ネットワーク管理センター（ＮＭＣ）９と、衛星制御センター（ＳＣＣ）１０と、追跡・遠隔測定・制御局（ＴＴ&Ｃ）１１とを具備する。複数のＳＡＮ１ａ，１ｂ，１ｃは、高容量デジタルネットワーク２（バックボーンネットワーク）によって相互結合されている。ＧＷ５ａ，５ｂ，５ｃは、ＳＡＮ１ａ，１ｂ，１ｃと他の従来の地上ベースの電話ネットワーク６，７，８との間の接続を提供する。ＮＭＣ９とＳＣＣ１０とＴＴ&Ｃ１１とは、低容量デジタルネットワーク１２によって相互結合されている。低容量デジタルネットワーク１２は、また、バックボーンネットワーク２へ接続されている。他の地上ベースの電話ネットワーク６，７，８は、公衆交換電話ネットワーク（ＰＳＴＮ）６と公衆交換データネットワーク（ＰＳＤＮ）７と公衆地上移動ネットワーク（ＰＬＭＮ）８とを含む。ＰＳＴＮ６は、従来の電話器１３への接続が成されることを可能とする。

【００２６】ＳＣＣ１０とＴＴ&Ｃ１１とは、衛星３ａ，３ｂの動作（例えば、送信電力レベルの設定とトランスポンダー入力の同調と）を、ＮＭＣ９による指図の通りに制御する。衛星３ａ，３ｂからの遠隔測定信号は、「衛星３ａ，３ｂが正確に機能している」ということを保証するために、ＴＴ&Ｃ１１によって受信され、かつ、ＳＣＣ１０によって処理される。

【００２７】図１に示されるように、使用者端末ＵＴ４ａは、また、従来の地上ベースの移動ネットワークＰＬＭＮ８と通信できる。ＰＬＭＮ８は、（使用者端末ＵＴ４ａとの二重通信方式リンク１５を確立する）トランシーバー局１４を具備する。この例では、ＰＬＭＮ８は、ＧＳＭネットワークである。

【００２８】ＧＳＭのより完全な理解のためには、欧州遠距離通信学会（ＥＴＳＩ）によって発行されている様々なＧＳＭ勧告を参照されたい。より読みやすい概観としては、M.Mouly とM-B.Pautetとによる”The GSM System for Mobile Communications”（1992年、Cell & Sys 、ISBN:2-9507190-0-7）も参照されたい。

【００２９】衛星ネットワークは、世界中に及ぶ受信可能範囲を提供するように設計されている。そのため、衛星３ａ，３ｂは、衛星群の一部を形成する。該衛星群は、いくつかの軌道内に配置されていてもよい。一例では、５つの衛星の２つの軌道が使用される。これらの衛星は、地球の表面の大部分の受信可能範囲を提供するように示されることができる。該受信可能範囲では、１０°の衛星上昇角度に対して、１つの衛星が、ＵＴによって、全ての時間においてアクセスされることができ、かつ、２つの衛星が、少なくとも８０％の時間に渡って、アクセスされることができる。その結果、システムの多様性を提供する。追加の冗長性と多様性とを提供するために、更なる衛星が衛星群内に具備されてもよい。

【００３０】本発明は、特定の軌道半径に限定されるものではないが、衛星は、（例えば、１０３５５ｋｍの軌道半径を有する）中間地球軌道（ＭＥＯ）群内に配置されている。この実施形態では、衛星３ａ，３ｂは、共通の軌道内に示されており、かつ、該衛星は、各ＳＡＮ１ａ，１ｂ，１ｃのアンテナ配列１６によって追跡される。一般的に、各ＳＡＮは、衛星群の個々の衛星を追跡するために４つのアンテナ（と１つの予備アンテナと）を具備する。ＳＡＮは、連続した受信可能範囲を提供するために、地球の方々に間隔をあけて置かれている。示された実施形態では、ＳＡＮ１ａはヨーロッパに配置されており、一方、ＳＡＮ１ｂはアフリカに配置されており、かつ、ＳＡＮ１ｃはアメリカに配置されており、かつ、他のＳＡＮは他の場所に配置されている。図１では、ＳＡＮ１ｂは、衛星３ｂを介して使用者端末ＵＴ４ｂと通信していることが示されている。衛星ネットワークの更なる詳細については、英国特許公開第２２９５２９６号公報を参照されたい。

【００３１】衛星３ａ，３ｂは、非静止軌道内に存在し、かつ、ヒューズ（Hughes）ＨＳ６０１のような従来の衛星を一般に具備する。該衛星３ａ，３ｂは、英国特許公開第２２８８９１３号公報に記載されているような特徴を具備してもよい。各衛星３ａ，３ｂは、衛星の下の（地球上の）フットプリントをカバーする無線ビームの配列を生成するように配置されている。各ビームは、英国特許公開第２２９３７２５号公報に記述されているように、多数の異なる周波数チャネルおよびタイムスロットを具備する。故に、該ビームは、隣接するセルラーエリアを提供する。該セルラーエリアは、従来の地上ベースの移動電話ネットワークのセルに対応する。

【００３２】電話呼の間、使用者端末ＵＴ４ａ，４ｂは、（ダウンリンクチャネルとアップリンクチャネルとを具備する）全二重通信方式チャネルを介して、衛星３ａ，３ｂと通信する。該チャネルは（呼の開始時に割り当てられた周波数上または呼の間に再割り当てされた周波数上に）ＴＤＭＡタイムスロットを具備する。

【００３３】図２を参照すると、ＳＡＮ１ａおよび（局所的な）ＰＬＭＮ８の構成が、より詳細に示されている。ＳＡＮ１ａは、衛星基地局ＳＢＳ２０からなる。ＳＢＳ２０は、衛星を追跡するための５つの皿状アンテナ１６へ結合されている。ＳＢＳ２０は、増幅器とマルチプレクサとデマルチプレクサと符復号器とを伴う送信／受信回路を具備する。移動衛星スイッチングセンターＭＳＳＣ２１は、ＳＢＳ２０へ結合されており、かつ、衛星ビジターロケーションレジスタVLR_{SAT}２２を具備

する。ＭＳＳＣ２１は、通信信号を、バックボーンネットワーク２およびＳＢＳ２０へ結合する。それによって、個々の電話呼が（バックボーンネットワーク２および二重通信方式リンクを通して、衛星３ａを介して）移動端末ＵＴ４ａへ確立されることを可能とする。

【００３４】また、ＭＳＳＣ２１は、（図１に示されるＰＳＤＮ７およびＰＳＴＮ６と）ＰＬＭＮ８への出力接続を提供するために、ゲートウエーＧＷ５ａへ接続されている。「全てのＳＡＮは、登録されている加入者の記録を保持するために、個々のＶＬＲ$_{SAT}$ を伴う類似の構成である」ということが理解される。

【００３５】ＶＬＲ$_{SAT}$２２ は、現在登録されている各々の加入者の記録（即ち、信号通信のためにＳＡＮ１ａを使用している各使用者の同一性）を保持する。

【００３６】ＭＳＳＣ２１は、信号を該信号の目的地へ適切に送るために、アンテナ１６からの到来通信信号上のアドレスに応答する。

【００３７】図３を参照すると、衛星サービス設備は、データベースを使用する。該データベースは、ここでは、衛星ホームロケーションレジスタ（ＨＬＲ$_{SAT}$）２３ として参照される。ＨＬＲ$_{SAT}$２３ は、各移動ユーザーに関する契約記録を具備する。該記録は、使用者の同一性を含む。該同一性は、国際的移動加入者アイデンティティ（International Mobile Subscriber Identity：ＩＭＳＩ）と、契約の現在状態と、ＵＴの現在の登録位置とを含む。ＨＬＲ$_{SAT}$ は、（図１に示される）ＮＭＣ９に配置されてもよく、または、ＳＡＮ１ａ，１ｂ，１ｃ内に分散配置されてもよい。

【００３８】衛星サービス設備は、また、サーバーを使用する。該サーバーは、ここでは、料金前払サーバー（ＰＰＳ）２４として参照される。ＰＰＳ２４の動作は、以下に詳細に説明される。ＨＬＲ$_{SAT}$ を伴うので、ＰＰＳ２４の位置は、融通がきく。例えば、ＰＰＳ２４は、（図１に示される）ＮＭＣ９に配置されてもよく、または、ＳＡＮ１ａ，１ｂ，１ｃの内の１つに配置されてもよい。

【００３９】図２を再び参照すると、この例におけるＰＬＭＮ８は、ＵＫベースのＧＳＭネットワークを具備し、かつ、多数の基地トランシーバー局ＢＴＳ３０，３１，３２を具備する。ＢＴＳ３０，３１，３２は、それ自体がよく知られた方法でセルラーネットワークをサポートするために、地理的に間隔をあけて配置されている。ＢＴＳ３０は、関連するアンテナ１４を伴って示されている。該アンテナ１４は、地上線によって、基地局コントローラＢＳＣ３３へ接続されている。「複数のＢＴＳ３０，３１，３２が、それ自体がよく知られた方法でＢＳＣ３３へ接続されている」ということが理解される。ＢＳＣ３３は、移動スイッチングセンターＭＳＣ３４へ接続されている。ＭＳＣ３４は、移動ネットワーク内の呼を経路決定できる。また、ＭＳＣ３４は、該呼を、それ自体がよく知られた方法で、ゲートウエーＧＭＳＣ３５を通して、線３６上で、従来のＰＳＴＮ６へ送ることができる。または、ＭＳＣ３４は、該呼を、線３７上で、ゲートウエーＧＷ５ａを通して、衛星ネットワークへ送ることができる。

【００４０】地上ベースのネットワーク８に対するホームロケーションレジスタＨＬＲ３８は、ＧＭＳＣ３５へ結合されて提供される。従来の方法では、ＨＬＲは、ネットワーク８に加入している使用者のＩＭＳＩの記録を保持する。ビジターロケーションレジスタＶＬＲ３９は、ネットワーク８に一時的に登録された加入者の記録を保持する。例えば、ＵＫに位置するＰＬＭＮ８では、他の国（例えば、ドイツ）内のＧＳＭネットワークへの加入者は、ＵＫ内にいる間、一時的に、局所的に登録される。従来の方法では、電話使用情報は、ＶＬＲ３９およびＧＭＳＣ３５から、ドイツのネットワーク（不図示）へ、課金目的のために中継される。他のタイプのネットワークへのＰＬＭＮの相互連結は、インターワーキングファンクション（Interworking function）ＩＷＦ４０ の設備によって、容易にされる。ＩＷＦ４０は、ＧＳＭ送信特性を、接続されたネットワークの送信特性に適応させるよう、構成されている。ＧＳＭのＰＬＭＮと衛星移動電話システムとの間におけるＩＷＦの実行の詳細については、我々（出願人）の係争中の出願97302222.1”Interworking between Telecommunications Networks”を参照されたい。

【００４１】図４および図５を参照すると、移動使用者端末ＵＴ４ａは、局所的な地上セルラーネットワークおよび衛星ネットワークの両方を伴って動作するように構成されている。故に、図２に示される例では、ＵＴ４ａは、地上ベースのＧＳＭプロトコルと衛星ネットワークプロトコルとのいずれかに従って動作できる。図４に示されるように、ＵＴ４ａは、移動送受器を具備する。該移動送受器は、デュアルモード動作が可能である。該移動送受器は、地上ベースのセルラーネットワーク９を伴った使用のための従来のＧＳＭ回路を、衛星ネットワークを伴った使用のための類似回路と共に、具備する。図４に示されるように、送受器は、マイクロフォン５０とラウドスピーカー５１とバッテリ５２とキーパッド５３とアンテナ５４とディスプレイ５５とを具備する。携帯装置ＵＴ４ａは、また、加入者識別モジュール（ＳＩＭ）５６を具備する。ＳＩＭ５６は、よく知られたサイズ（クレジットカードサイズ）を有するスマートカードであってもよく、または、ＩＳＯ規格に従ったより小さなプラグインモジュールであってもよい。ＵＴ４ａの回路構成は、図５において、ブロック図形式で示される。ＳＩＭ５６（例えば、ＳＩＭスマートカード）は、ＳＩＭカードリーダー５７内に収納される。ＳＩＭカードリーダー５７は、コントローラ５８（一般的には、マイクロプロセッサ）に結合されている。マイクロフォン５０

およびラウドスピーカー５１は、第１符復号器５９ａおよび第２符復号器５９ｂへ結合されている。第１符復号器５９ａおよび第２符復号器５９ｂは、従来の無線インターフェース６０へ結合されている。無線インターフェース６０はアンテナ５４へ結合されている。それによって、通信信号を（本質的によく知られた方法で）送受信する。フェイズ２＋コンプライアントＧＳＭシステム（Phase 2+ compliant GSM system ）において、ＳＩＭ５６は、ＳＩＭアプリケーションツールキット（SIM Application Toolkit ）として知られるソフトウェアを具備する。ＳＩＭアプリケーションツールキットは、ＳＩＭによる（ＵＴ機能の）洗練された制御を可能にする。

【００４２】図６を参照すると、ＳＩＭ５６は、メモリＭ１を具備する。メモリＭ１は、ＩＭＳＩを記憶する。ＩＭＳＩは、ＧＳＭネットワーク８と衛星ネットワークとの両方で使用される。該メモリは、また、上記ＧＳＭ勧告に従う契約認証と通信暗号化とのために、暗号化アルゴリズムと認証アルゴリズムと暗号化キーＫｉとを記憶する。故に、ＵＴ４ａは、（この技術分野でよく知られた）従来のＧＳＭ登録技術に従って、いずれのネットワークにも自己を登録できる。該認証手続および（その後に続く）データの暗号化／解読の更なる詳細については、M.Mouly とM-B.Pautetとによる”The GSM System for Mobile Communications”（1992年、Cell & Sys ）の第４７７～４９２頁目を参照されたい。

【００４３】先に述べられたように、衛星ネットワークおよび地上ベースのネットワークは、使用者によって決定された基準に従って、自動的に選択される。しかしながら、この例では、説明を簡単にするために、衛星ネットワークおよび地上ベースのネットワークは、キーパッド５３上のキーの使用によって、手動で選択される。ＧＳＭネットワークが選択されると、コントローラ５８は、無線インターフェース６０を、地上ベースのＧＳＭネットワーク８に対して適切な周波数で動作するように設定し、かつ、（ＧＳＭネットワークに対して適切な）符復号器５９ａが選択される。他に、もし、衛星ネットワークを選択するようにキーパッド５３が操作されたならば、コントローラ５８は、無線インターフェース６０を、衛星ネットワークに対して適切な周波数およびプロトコルへ合わせるよう動作し、かつ、（衛星ネットワークに対して適切な）符復号器５９ｂが選択される。故に、ＧＳＭネットワークが選択されると、通信は、（図２に示される）二重通信方式リンク１５上で起こり、一方、衛星ネットワークが選択されると、通信は、衛星３ａを介した二重通信方式リンク上で起こる。

【００４４】図７を参照すると、料金前払ＩＣＯ加入者によって生成された呼の経路決定が詳細に考察されている。該ＩＣＯ加入者は、移動先のＧＳＭネットワーク内におり、使用者端末ＵＴ４ａを使用して、遠く離れたＰＳＴＮ６内の送受器へ電話をかけている。料金前払加入者は、料金前払ＳＩＭ５６を有している。料金前払ＳＩＭ５６は、例えば、契約番号に電話をかけることによって、かつ、希望する量のクレジットを購入するために（クレジットカードのような）適切な支払手段を使用することによって、料金請求されることができる。フェイズ２＋ＳＩＭツールキットコンプライアントＳＩＭカード（Phase 2+ SIM Toolkit compliant SIMcard ）のような料金前払ＳＩＭ５６は、ＵＴ４ａを制御するために、本発明に従ってセットアップされる。

【００４５】概して言えば、料金前払ＳＩＭ５６の機能は、クレジット照合確認メッセージを開始することと、許容呼期間を管理することと、ＵＴ操作を制御することとを含む。これらは、以下に、より詳細に説明される。

【００４６】ＵＴ４ａがスイッチを入れられると、ＵＴ４ａは、該ＵＴ４ａのホームネットワークからサービスを得ることを試みる。もし、例えば、ＵＴ４ａが（ＰＬＭＮ８のような）他のネットワークのサービスエリアへ移動しているために、該サービスを得ることができないならば、第１ステップ（ｓ１）は、ＵＴ４ａが（それ自体がよく知られた方法で）ＰＬＭＮ８に関連するＶＬＲ３９へ自己を登録することである。登録手続の結果として、ＳＩＭは、移動先ネットワークＰＬＭＮ８の同一性を得る。

【００４７】その後、加入者が（ＰＬＭＮ８を使用して）電話をかけたい場合、該加入者は、ＵＴキーパッド５３において、ターゲット電話１３の番号を入力し、かつ、キーパッド上の’ＳＥＮＤ’ボタンを押す（ｓ２）。ＳＩＭ５６は、ＵＴ４ａが直ちに電話をかけることを禁止し、かつ、代わりに、使用者に適切なメッセージ（例えば、「クレジット照合中……お待ち下さい」）を表示することを、ＵＴ４ａに指示する（ｓ３）。そして、ＳＩＭは、標準ＧＳＭアンストラクチャードサプリメンタリサービスデータ（standard GSM Unstructured Supplementrary Service Data ：ＵＳＳＤ）サービスを使用してメッセージをホームネットワークへ送信することを、ＵＴに指示する。ＵＳＳＤサービスは、全てのＧＳＭプロバイダによってサポートされている。ＵＳＳＤメッセージの内容は、移動先ネットワークの同一性とＩＭＳＩとダイヤル番号とを含む。該メッセージは、ホームネットワークによって決定された料金前払クレジット確認／保安プロトコルに従って、符号化される。

【００４８】ＵＳＳＤメッセージは、ホームネットワークＭＳＳＣ２１によって受信される。ホームネットワークＭＳＳＣ２１は、メッセージを料金前払サーバー（ＰＰＳ）２４へ送る（ｓ５）ように構成されている。ＰＰＳ２４は、各料金前払加入者に対するクレジット記録を含むデータベースを具備する。ＰＰＳは、例えば、専用コンピュータ上に実現される。

【００４９】ＰＰＳ２４は、供給されたＩＭＳＩ情報に基づいて加入者を識別し、かつ、該加入者に対応するク

レジット記録を検索する（ｓ６）。そして、ＰＰＳ２４は、移動先ネットワーク同一性とダイアル番号情報と現在時刻情報とを使用して、該呼に適応する（ＰＬＭＮ８の）料金表を決定する（ｓ７）。該料金表情報は、ネットワークオペレータ間の標準移動契約に基づいて得られる。

【００５０】利用可能なクレジットと適応可能な料金表とが分かると、ＰＰＳは、ネットワーク８上に生成されるべき特定の呼に対して許可される呼期間を計算する（ｓ８）。この情報は、ステップｓ９において、ＵＳＳＤメッセージ内で、ＭＳＳＣ２１を介して、ＵＴおよびＳＩＭへ送信される。

【００５１】ＳＩＭは、移動先ネットワーク８上での呼を可能にし、かつ、通常表示へ戻ることをＵＴへ指示する（ｓ１０）。該通常表示は、例えば、ダイヤルされている番号を表示する。そして、接続が確立すると、ＳＩＭは、内部タイマを起動する（ｓ１１）。該内部タイマは、ＰＰＳ２４によって供給された時間からカウントダウンする。ＳＩＭは、この段階で可能な様々な表示を示すこと（例えば、残存している呼時間を表示すること）を、ＵＴに指示してもよい（明確には示されていないステップ）。

【００５２】タイマが呼の期間を終了すると、ＳＩＭは、呼を終了することを、ＵＴに指示し（ｓ１２）、かつ、（呼期間を示す）ＵＳＳＤメッセージをＭＳＳＣ２１へ返送することを、ＵＴに指示する（ｓ１４）。もし、タイマが終了する前に呼が終わるならば、ＳＩＭはタイマを停止し（ｓ１３）、かつ、タイマ終了の場合と同様に、（呼期間を示す）ＵＳＳＤメッセージをＭＳＳＣ２１へ返送することを、ＵＴに指示する（ｓ１４）。いずれの場合にも、ＭＳＳＣ２１は、ＵＳＳＤメッセージをＰＰＳ２４へ送る（ｓ１５）。ＰＰＳ２４は、残存呼時間を計算し、かつ、該残存時間を（加入者にクレジットされている）クレジット量に変換する（ｓ１６）。ＳＩＭ５６は、料金前払クレジットを料金再請求するために、（ホームネットワーク番号への呼を除いては）更なる呼の試みを見合わせる。

【００５３】他に、ＰＰＳ２４がＳＩＭに利用可能な呼時間を知らせると、ＰＰＳ２４は、ステップｓ８において、クレジット記録をゼロに設定し、かつ、「期限満了になっていない時間が幾分残っている」ということを示すためにセットアップされるＵＳＳＤメッセージを受信する場合のみ、クレジット記録をリセットする。このことは、もし、呼時間が終了するならば、ＵＴがＵＳＳＤメッセージを返送する必要を避ける。

【００５４】本発明は（加入者が該加入者のホームネットワーク以外のネットワークへ移動している間における）リアルタイムクレジット照合の点において説明されたが、「クレジット計算は、別のネットワーク上の別の料金表を考慮して、前もって実行されることができる」ということも予見される。そして、利用可能時間情報は、使用者端末が他のネットワークへ（引き続き）移動するときの使用のために、ＳＩＭカード内に記憶されることができる。

【００５５】他に、呼のセットアップの度にクレジット照合を実行するよりもむしろ、クレジット照合は、１日毎にまたは他の周期に基づいて、実行されてもよい。例えば、例えば、ＵＴがスイッチを入れられると、クレジット詳細がＳＩＭカードに一時的に記憶される。そして、日中に生成された呼に対しては、ＳＩＭカードが、料金前払サーバーの代理を行い、一日の終わりにＵＴがスイッチを切られると、料金前払サーバーを更新するだけである。

【図面の簡単な説明】

【図１】　本発明による衛星遠距離通信システムの一例を示すブロック図である。

【図２】　衛星ネットワークおよび地上セルラーネットワークの一例を示すブロック図である。

【図３】　衛星ネットワーク内の料金前払サーバーの設備の一例を示すブロック図である。

【図４】　移動使用者端末の一例を示す概要図である。

【図５】　移動使用者端末の回路構成例を示すブロック図である。

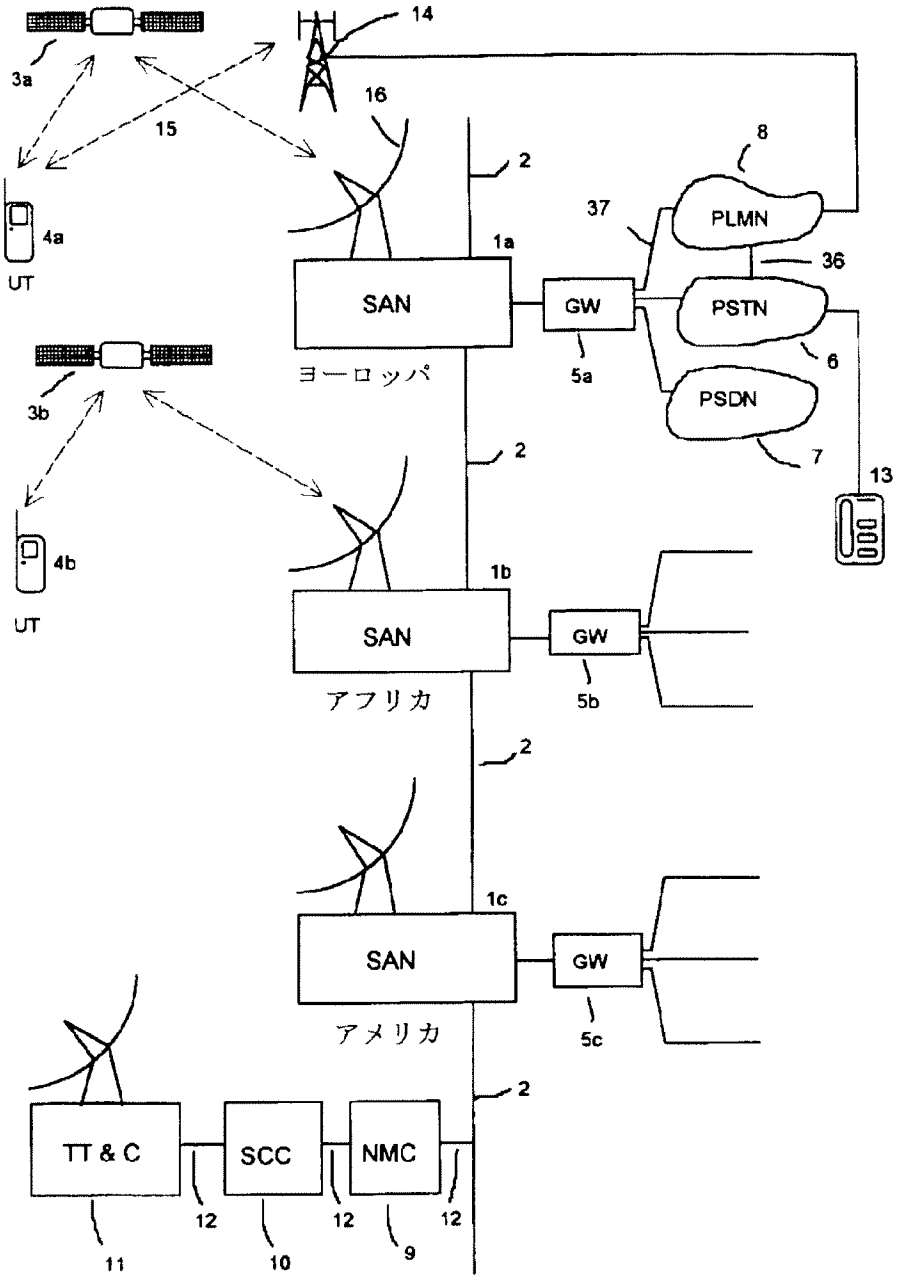
【図６】　ＳＩＭカードの一例を示すブロック図である。

【図７】　本発明によるクレジット照合手続の一例を示すフローチャートである。

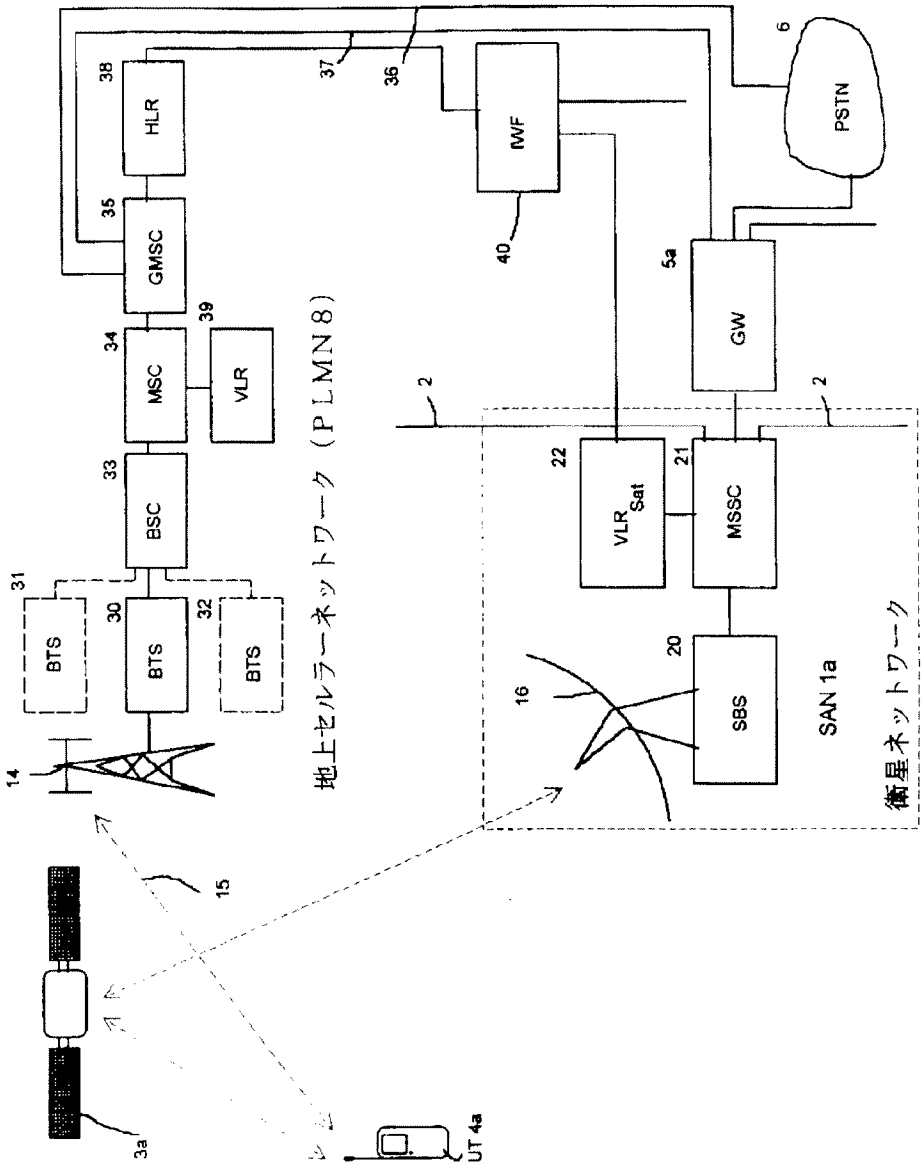
【符号の説明】

１ａ，１ｂ，１ｃ……衛星アクセスノード、２……バックボーンネットワーク、　３ａ，３ｂ……衛星、４ａ，４ｂ……使用者端末、　５ａ，５ｂ，５ｃ……ゲートウエー、６……公衆交換電話ネットワーク、　７……公衆交換データネットワーク、８……公衆地上移動ネットワーク、　９……ネットワーク管理センター、１０……衛星制御センター、　１１……追跡・遠隔測定・制御局

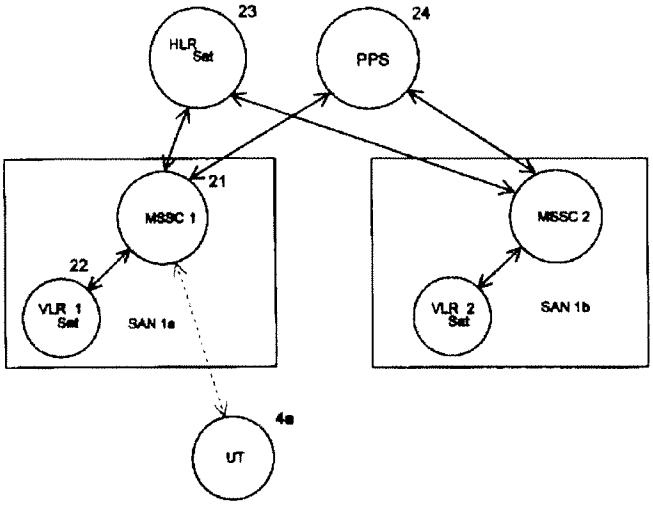
【図１】


14
3a
16
15
2
8
37
PLMN
4a
UT
1a
SAN
GW
PSTN
36
ヨーロッパ
5a
6
3b
PSDN
7
13
2
4b
UT
1b
SAN
GW
アフリカ
5b
2
1c
SAN
GW
アメリカ
5c
2
TT & C
SCC
NMC
12
12
12
11
10
9

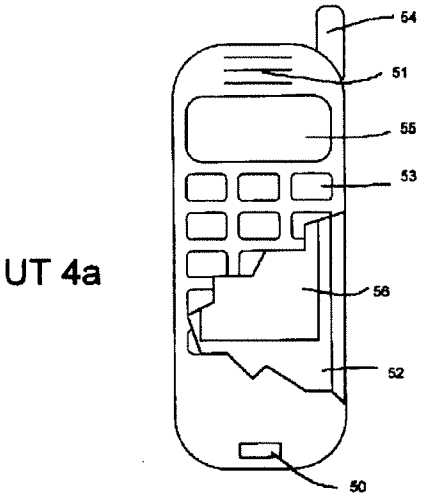
【図２】


地上セルラーネットワーク（ＰＬＭＮ８）
衛星ネットワーク
SAN 1a
HLR
GMSC
MSC
VLR
BSC
BTS
BTS
BTS
IWF
PSTN
GW
VLR Sat
MSSC
SBS
UT 4a
3a
14
15
16
2
2
5a
6
20
21
22
30
31
32
33
34
35
36
37
38
39
40

【図３】

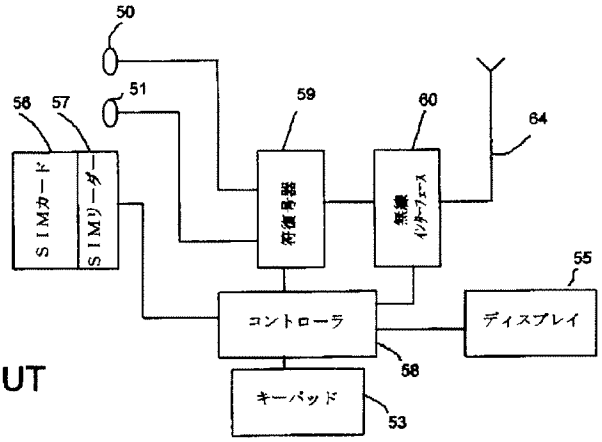


【図４】

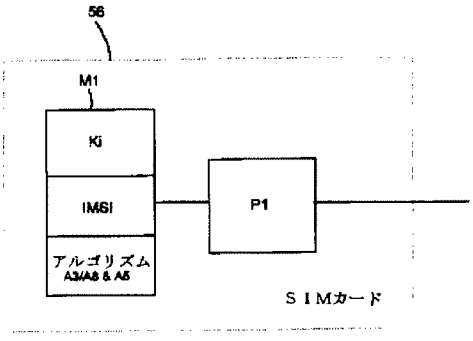


UT 4a

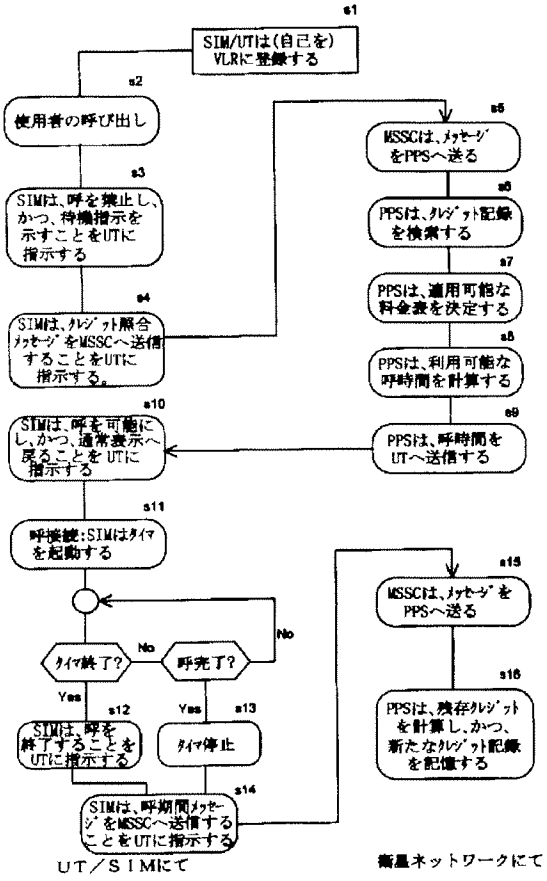
【図５】



【図６】



【図７】


s1
SIM/UTは(自己を)VLRに登録する
s2
使用者の呼び出し
s3
SIMは、呼を禁止し、かつ、待機指示を示すことをUTに指示する
s4
SIMは、クレジット照合メッセージをMSSCへ送信することをUTに指示する。
s5
MSSCは、メッセージをPPSへ送る
s6
PPSは、クレジット記録を検索する
s7
PPSは、適用可能な料金表を決定する
s8
PPSは、利用可能な呼時間を計算する
s9
PPSは、呼時間をUTへ送信する
s10
SIMは、呼を可能にし、かつ、通常表示へ戻ることをUTに指示する
s11
呼接続:SIMはタイマを起動する
タイマ終了?
No
呼完了?
No
Yes
Yes
s12
SIMは、呼を終了することをUTに指示する
s13
タイマ停止
s14
SIMは、呼期間メッセージをMSSCへ送信することをUTに指示する
s15
MSSCは、メッセージをPPSへ送る
s16
PPSは、残存クレジットを計算し、かつ、新たなクレジット記録を記憶する
UT／ＳＩＭにて
衛星ネットワークにて

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-115353
(43)Date of publication of application : 21.04.2000

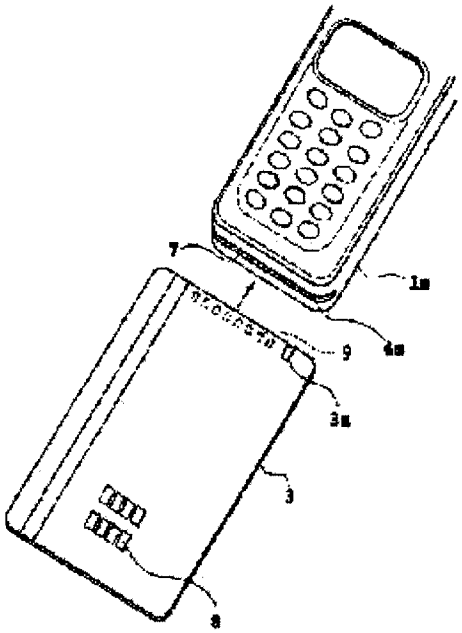
(51)Int.Cl. H04M 1/675
G06F 3/08
H04B 7/26
H04M 1/725
H04M 11/00

(21)Application number : 10-276008
(22)Date of filing : 29.09.1998

(71)Applicant : NTT MOBIL COMMUNICATION NETWORK INC
(72)Inventor : FURUSE MASAHIRO
HAMADA KATSUNORI
WAKABAYASHI TATSUAKI
ISHIKAWA HIDETOSHI

(54) MOBILE COMMUNICATION TERMINAL

(57)Abstract:
PROBLEM TO BE SOLVED: To easily read/write data or the like from/to an SIM mounted on a mobile communication terminal, without removing the SIM.
SOLUTION: Eight terminals of a connection section 4 of a main body 1a is connected electrically to 8 terminals of a card 3, by inserting (mounting) one end of the card 3 to a groove structure of the connection section 4 in a way such that a projection 4a of the main body 1a is inserted into a notch 3a of the card 3. Since a SIM 6 in a radio device 1 is connected electrically to a connection section 8 of the cad 3, data are read from/written in the SIM 6 via the connection section 8 by inserting the card 3 to a reader/writer, while keeping this state (mounting the SIM 6 in the radio device 1).



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－115353
（P2000－115353A）
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
Ｈ０４Ｍ　1/675		Ｈ０４Ｍ　1/66	Ｅ	５Ｂ０６５
Ｇ０６Ｆ　3/08		Ｇ０６Ｆ　3/08	Ｃ	５Ｋ０２７
Ｈ０４Ｂ　7/26		Ｈ０４Ｍ　1/72	Ｂ	５Ｋ０６７
Ｈ０４Ｍ　1/725		11/00	３０２	５Ｋ１０１
11/00	３０２	Ｈ０４Ｂ　7/26	Ｍ	

審査請求　未請求　請求項の数５　ＯＬ　（全５頁）

(21)出願番号　特願平10－276008

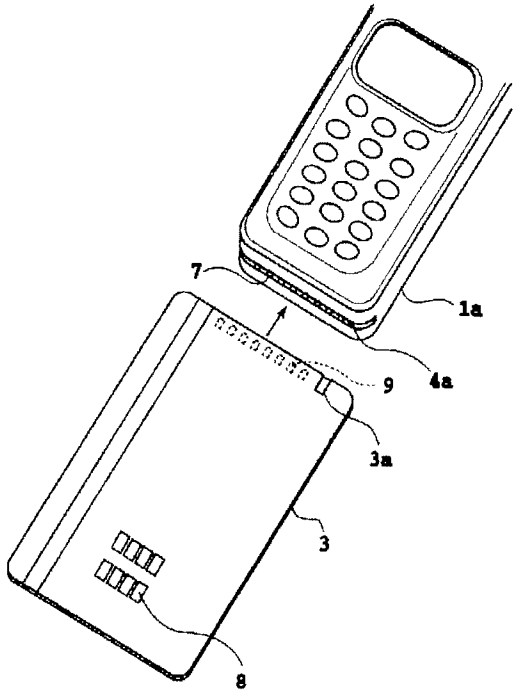
(22)出願日　平成10年９月29日(1998.9.29)

(71)出願人　392026693
エヌ・ティ・ティ移動通信網株式会社
東京都港区虎ノ門二丁目10番１号
(72)発明者　古瀬　正浩
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(72)発明者　濱田　克徳
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(74)代理人　100077481
弁理士　谷　義一　（外３名）

最終頁に続く

(54)【発明の名称】　移動通信端末

(57)【要約】
【課題】　移動通信端末に装着されたＳＩＭに対するデータ等の読み書きをＳＩＭを取り外すことなく容易に行うこと。
【解決手段】　カード３の切れ込み３ａに本体１ａの突起４ａが挿入されるようにして接続部４の溝構造にカード３の一端部を挿入（装着）することによって、本体１ａの接続部４の８個の端子とカード３の８個の端子とが電気的に接続される。これによって、無線機１内のＳＩＭ６とカード３の接続部８とが電気的に接続されるので、この状態のまま（無線機１内にＳＩＭ６を装着したまま）、カード３をリーダ・ライタに挿入することによって、接続部８を介して、ＳＩＭ６に対してリーダ・ライタからデータの読み書きを行うことができるようになる。



1

【特許請求の範囲】

【請求項１】　所定の情報が記憶された記憶手段が装着される移動通信端末であって、ＩＣカードとほぼ同形状であって所定の位置に信号の入出力が可能な端子を持つカード状連結手段と接続するための接続部を有し、前記接続部を介して前記記憶手段と前記端子とが電気的に接続されることを特徴とする移動通信端末。

【請求項２】　請求項１において、
前記記憶手段はＳＩＭであることを特徴とする移動通信端末。

【請求項３】　所定の情報が記憶された記憶手段が装着される移動通信端末であって、ＩＣカードとほぼ同形状であって所定の位置に信号の入出力が可能な端子を持つカード状のカバーを有し、前記記憶手段と前記端子とが電気的に接続されていることを特徴とする移動通信端末。

【請求項４】　請求項３において、
前記記憶手段はＳＩＭであることを特徴とする移動通信端末。

【請求項５】　請求項３または４において、
前記カバーは、折り畳み又はスライド可能であることを特徴とする移動通信端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、加入者情報等が記憶されたＩＣカード（以下、ＳＩＭ：Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）を搭載した移動通信端末に関する。

【０００２】

【従来の技術】ＳＩＭはフルサイズのＩＣカードよりも小型であり、従来、加入者情報等が記憶されたＳＩＭが搭載された移動通信端末（携帯電話、ＰＨＳ等）が知られている。

【０００３】

【発明が解決しようとする課題】上述のような移動通信端末においては、ＳＩＭはその通信端末内のソケットに装着されており、このＳＩＭ内の加入者情報あるいはこれに加えてアプリケーションを利用する際には、外部のリーダ・ライタにＳＩＭを接続しなければならない。そのためには、ＳＩＭを移動通信端末から取り外さなければならない。

【０００４】さらに、小型なＳＩＭを移動通信端末から取り外すことは容易ではなく、取り外したＳＩＭを移動通信端末内のソケットに再び装着することも容易ではない。また、ＳＩＭの装着、取り外しは、ＳＩＭを移動通信端末内の所定のソケットに対して抜き差しすることによって行うが、このような抜き差しを行って、外部のリーダ・ライタと接続して読み書きを行うと、その接触部が著しく劣化してしまう。

【０００５】そこで本発明の目的は、以上のような問題

2

を解消した移動通信端末を提供することにある。

【０００６】

【課題を解決するための手段】上記目的を達成するため、請求項１の発明は、所定の情報が記憶された記憶手段が装着される移動通信端末であって、ＩＣカードとほぼ同形状であって所定の位置に信号の入出力が可能な端子を持つカード状連結手段と接続するための接続部を有し、前記接続部を介して前記記憶手段と前記端子とが電気的に接続されることを特徴とする。

【０００７】また請求項２の発明は、請求項１において、前記記憶手段はＳＩＭであることを特徴とする。

【０００８】さらに請求項３の発明は、所定の情報が記憶された記憶手段が装着される移動通信端末であって、ＩＣカードとほぼ同形状であって所定の位置に信号の入出力が可能な端子を持つカード状のカバーを有し、前記記憶手段と前記端子とが電気的に接続されていることを特徴とする。

【０００９】さらに請求項４の発明は、請求項３において、前記記憶手段はＳＩＭであることを特徴とする。

【００１０】さらに請求項５の発明は、請求項３または４において、前記カバーは、折り畳み又はスライド可能であることを特徴とする。

【００１１】

【発明の実施の形態】図１は本発明の第１の実施形態の正面図、図２は同背面図である。

【００１２】１は移動通信端末を構成する無線機であって、その本体１ａの上部にはアンテナ２が設けられており、また、本体１ａの下部には、後述するカード３と接続するための接続部４が設けられている。図１，図２は本体１ａの接続部４にカード３が装着された状態を示している。

【００１３】本体１ａの内部には、ソケット５が設けられており、このソケット５には加入者情報等が記憶されたＳＩＭ６が装着される（図２はソケット５に装着されていない状態のＳＩＭ６を示してある）。

【００１４】接続部４は、図３に示すようにカード３の一端部を緊密に挿入（装着）可能な溝構造を持っており、この溝の一方の内側に、カード３の８個の端子（後述）と電気的に接続するための８個の端子７が並設されている。この８個の端子７の各々はソケット５とリード線等で接続されている。

【００１５】カード３は、フルサイズのＩＣカードと同一サイズを持ち、後述するような接続部および端子を有するものであって、その内部にＩＣ等の電子部品は有していない。このカード３の材質は例えばＩＣカードのそれと同一であっても良い。また、カード３は、ＩＣカードのそれと同一位置にＩＣカード用のリーダ・ライタに装着してデータを読み書きするための８個の接触部からなる接続部８が設けられている。さらにカード３の長さ方向の一端部には無線機１の本体１ａの接続部４の８個

の端子と電気的に接続するための８個の端子９が並設されている。このカード３の一端部に設けられた８個の端子９の各々は接続部８の８個の接触部の各々とリード線等で接続されている。

【００１６】なお、カード３の一方の面側の一端の１箇所には切れ込み３ａが設けられており、これと対応するように、本体１ａの接続部４の溝の他方の内側１箇所に突起４ａが設けられている。

【００１７】したがって、カード３の切れ込み３ａに本体１ａの突起４ａが挿入されるようにして接続部４の溝構造にカード３の一端部を挿入（装着）することによって、本体１ａの接続部４の８個の端子とカード３の８個の端子とが電気的に接続される（切れ込み３ａに突起４ａが挿入されるので、カード３の裏表を逆にして挿入されることはない）。これによって、無線機１内のＳＩＭ６とカード３の接続部８とが電気的に接続されるので、この状態のまま（無線機１内にＳＩＭ６を装着したまま）、カード３をリーダ・ライタに挿入することによって、接続部８を介して、ＳＩＭ６に対してリーダ・ライタからデータの読み書きを行うことができるようになる。必要なデータ処理が終了したならば、カード３をリーダ・ライタから抜き出し、無線機１の本体１ａからカード３を外すことによって、無線機１を使用することができる。

【００１８】図４は本発明の第２の実施形態の正面図、図５は同背面図（詳細は後述するが、カバーを閉じた状態、即ち折り畳まれた状態）である。

【００１９】１０は移動通信端末を構成する無線機であって、その本体１０ａの上部にはアンテナ１１が設けられており、また、本体１０ａの下部には、本体１０ａのキーパッドを保護するカバー１２の下端が回動可能に取り付けられている。本体１０ａの内部には、ソケット５が設けられており、このソケット５には加入者情報等が記憶されたＳＩＭ６が装着される。また、カバー１２を閉じることによって、キーパッドは保護され、図４に示すようにカバー１２を開くことによって、後述のように本体１０ａ内のＳＩＭ６と、外部のリーダ・ライタとの間のデータのやり取りが可能となる。

【００２０】カバー１２は、フルサイズのＩＣカードと同一サイズを持ち、その内部にＩＣ等の電子部品は有していない。また、カバー１２は、ＩＣカードのそれと同一位置にＩＣカード用のリーダ・ライタに装着してデータを読み書きするための８個の接触部からなる接続部１３が設けられている。ソケット５と接続部１３の８個の接触部の各々とはリード線等で接続されている。これによって、無線機１０内のＳＩＭ６とカバー１２の接続部１３とが電気的に接続されることになる。

【００２１】したがって、カバー１２を開いた状態で（無線機１０内にＳＩＭ６を装着したまま）、カバー１２をリーダ・ライタに挿入することによって、接続部１３を介して、ＳＩＭ６に対してリーダ・ライタからデータの読み書きを行うことができるようになる。

【００２２】なお、カバー１２は折り畳み式としたが、そのほかにスライド式とすることもできる。

【００２３】

【発明の効果】以上説明したように本発明によれば、移動通信端末に装着された記憶手段（例えばＳＩＭ）に対するデータ等の読み書きを当該記憶手段を取り外すことなく容易に行うことができる。このため、例えば、前記記憶手段がＳＩＭの場合は、サービス利用手順が容易になるという効果が得られる。また、記憶手段を取り外さなくても済むので、その接点等の劣化を防ぐことができる。さらに、移動通信端末の一部としてＩＣカードと同形状のカバーを持つ場合は、信号の入出力を行う端子の劣化も防ぐことができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態の正面図である。

【図２】同背面図である。

【図３】同使用状態を示す斜視図である。

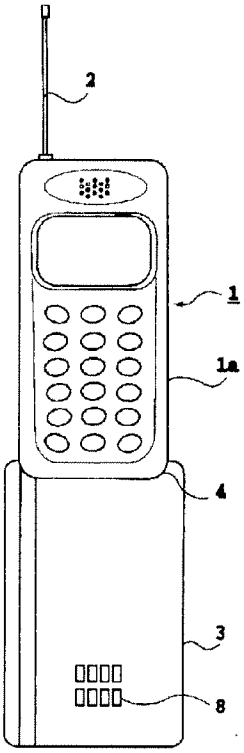
【図４】本発明の第２の実施形態の斜視図である。

【図５】同背面図である。

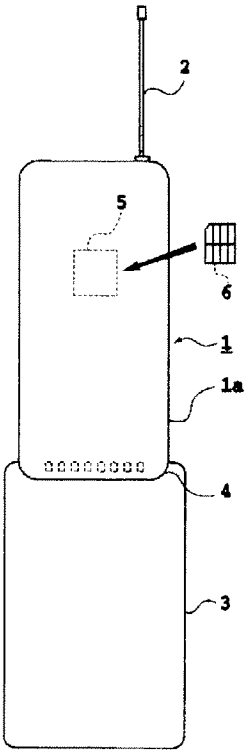
【符号の説明】

１　無線機
１ａ　本体
２　アンテナ
３　カード
４　接続部
５　ソケット
６　ＳＩＭ
７，９　端子
８　接続部

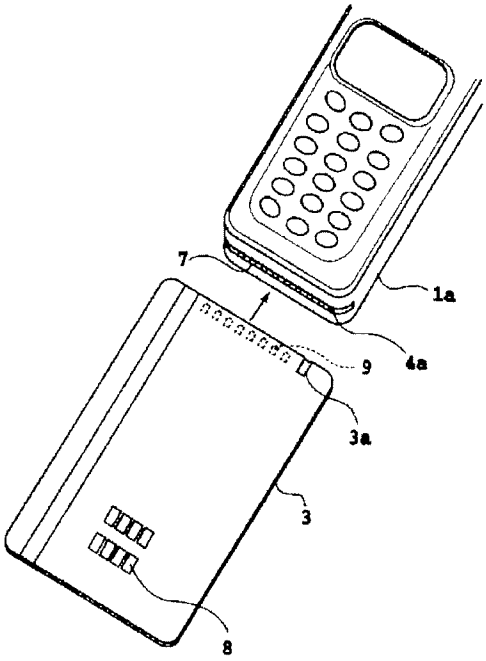
【図１】



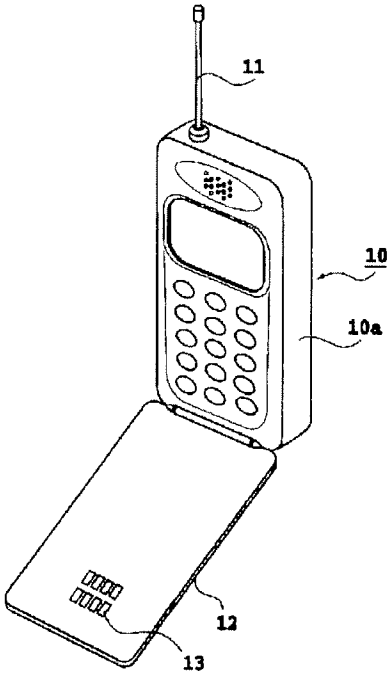
【図２】



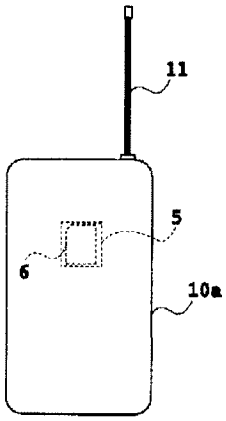
【図３】



【図４】



【図５】



フロントページの続き

(72)発明者　若林　達明
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(72)発明者　石川　秀俊
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内

Ｆターム(参考)　5B065 BA09 ZA11
5K027 AA11 BB02 BB09 HH23 KK07 MM03
5K067 AA34 BB04 BB21 DD51 EE03 FF02 FF23 HH23 KK15 KK17
5K101 KK20 NN40

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-279325
(43)Date of publication of application : 27.09.2002

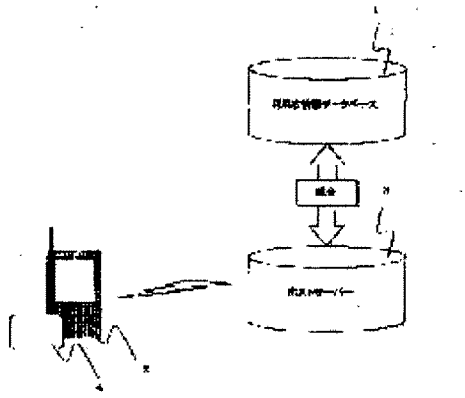
(51)Int.Cl. G06F 17/60
G06K 17/00

(21)Application number : 2001-076087
(22)Date of filing : 16.03.2001

(71)Applicant : JR EAST MECHATRONICS CO LTD
(72)Inventor : OGAWA KIYOTAKA
MORIYASU AKIYUKI
NANBU KEIICHI
SATO MASANOBU

(54) ELECTRONIC BUSINESS TRANSACTION SYSTEM USING CELLPHONE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a mobile electronic business transaction environment, used by a user at ease by taking security measures which are safer than the conventional one in a case of theft and loss in an electronic business transaction by a cellphone using SIM(subscriber identity module) card.
SOLUTION: This electronic business transaction system is provided with the cellphone 2 in which the SIM card 4 is inserted, a host server 3 on-line connected to the cellphone and having a function performing electronic business transaction, and users' information database 1 having a pre-registered combination of a cellphone number and SIM card identification information. When making transaction of the electronic business by on-line connecting to the cellphone, the host server collates the cellphone number and the SIM card identification information with the contents preregistered in the users database and, only when the collation result matches each other, will the value added information be downloaded to the cellphone.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－279325
（P2002－279325A）
(43)公開日　平成14年９月27日(2002.9.27)

(51)Int.Cl.'	識別記号	Ｆ Ｉ	テーマコード'(参考)
Ｇ０６Ｆ　17/60	４１４	Ｇ０６Ｆ　17/60	４１４　５Ｂ０５８
	１１２		１１２Ｈ
	１４６		１４６Ａ
	２２２		２２２
	３３０		３３０

審査請求　未請求　請求項の数１　ＯＬ　（全３頁）　最終頁に続く

(21)出願番号　特願2001－76087(P2001－76087)

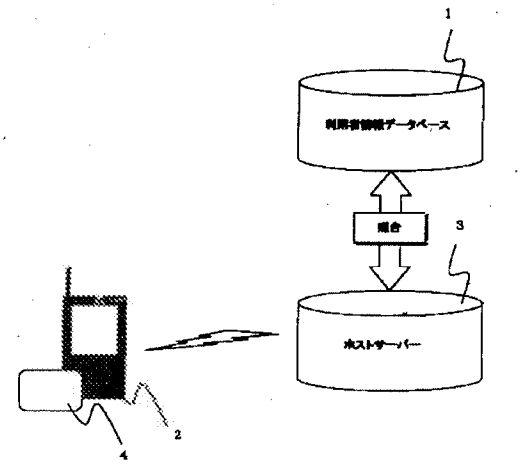
(22)出願日　平成13年３月16日(2001.3.16)

(71)出願人　593092482
ジェイアール東日本メカトロニクス株式会社
東京都港区芝浦３丁目８番10号
(72)発明者　小河清隆
東京都港区芝浦３丁目８番10号　ジェイアール東日本メカトロニクス株式会社内
(72)発明者　森安亮之
東京都港区芝浦３丁目８番10号　ジェイアール東日本メカトロニクス株式会社内
(74)代理人　100092495
弁理士　蛭川　昌信　（外７名）

最終頁に続く

(54)【発明の名称】　携帯電話を用いた電子商取引システム

(57)【要約】
【課題】　ＳＩＭカードを用いた携帯電話による電子商取引において、盗難、紛失時にこれまで以上のセキュリティ対策を施し、利用者が安心して使用できるモバイル電子商取引環境を提供する。
【解決手段】　ＳＩＭカード（４）がセットされる携帯電話機（２）と、携帯電話機とオンイライン接続して電子商取引を行う機能を有するホストサーバー（３）と、携帯電話番号およびＳＩＭカード識別情報の組み合わせが事前登録された利用者情報データベース（１）とを備え、ホストサーバーは、携帯電話機とオンイライン接続して電子商取引を行う際、携帯電話番号、ＳＩＭカード識別情報を利用者データベースに事前登録された内容と照合し、照合の結果一致する場合のみ付加価値情報を携帯電話機にダウンロードするようにしたものである。



1

【特許請求の範囲】

【請求項１】　ＳＩＭカードがセットされる携帯電話機と、携帯電話機とオンイライン接続して電子商取引を行う機能を有するホストサーバーと、携帯電話番号およびＳＩＭカード識別情報の組み合わせが事前登録された利用者情報データベースと、を備え、ホストサーバーは、携帯電話機とオンイライン接続して電子商取引を行う際、携帯電話番号、ＳＩＭカード識別情報を利用者データベースに事前登録された内容と照合し、照合の結果一致する場合のみ付加価値情報を携帯電話機にダウンロードすることを特徴とする携帯電話による電子商取引システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は携帯電話を用いた電子商取引システムに関する。

【０００２】

【従来の技術】現在、携帯電話によりホストサーバーにオンライン接続し、付加価値情報をダウンロードする種々なサービスが提案されている。このようなモバイルＥＣ（電子商取引）においては、盗難や紛失時のセキュリティ対策は、パスワードでの認証を行うのが一般的で、パスワードが一致しない場合にその携帯電話によるサービスを停止するというものでのある。

【０００３】ところで、携帯電話にＳＩＭ（加入者識別モジーュール）カードをセットし、携帯電話として機能させるＳＩＭカードシステムが提案され、欧州では既に普及し、日本においても近い将来、このシステムになると考えられている。ＳＩＭカードは機能的にＩＣカードと同等であり、１チップのＩＣにいろいろな個人情報を格納しており、さらに電子財布、定期券、チケット情報等いろいろな付加価値情報を格納することも提案されている。このようなＳＩＭカードを用いて携帯電話により電子商取引を行う際、カードの盗難や紛失時に対するセキュリティを確保することが必要である。

【０００４】

【発明が解決しようとする課題】しかしながら、従来の盗難、紛失時のセキュリティ対策は、パスワードでの認証が一般的で多くのパスワードは４桁であり、生年月日等の個人情報を用いることが多く、解読される危険性が高い。本発明はＳＩＭカードを用いた携帯電話による電子商取引において、盗難、紛失時にこれまで以上のセキュリティ対策を施し、利用者が安心して使用できるモバイル電子商取引環境を提供しようとするものである。

【０００５】

【課題を解決するための手段】本発明の携帯電話による電子商取引システムは、ＳＩＭカードがセットされる携帯電話機と、携帯電話機とオンイライン接続して電子商取引を行う機能を有するホストサーバーと、携帯電話番号およびＳＩＭカード識別情報の組み合わせが事前登録された利用者情報データベースとを備え、ホストサーバーは、携帯電話機とオンイライン接続して電子商取引を行う際、携帯電話番号、ＳＩＭカード識別情報を利用者データベースに事前登録された内容と照合し、照合の結果一致する場合のみ付加価値情報を携帯電話機にダウンロードすることを特徴とする。

2

【０００６】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しつつ説明する。図１は本発明の携帯電話による電子商取引システムを説明する概念図である。携帯電話機２には、ＳＩＭ（加入者識別モジーュール）カード４がセットされ、個人情報や電子商取引を行うための付加価値情報等の様々なデータが格納されている。ホストサーバー３は携帯電話機２とオンライン接続して電子商取引の処理を行い、取引が成立した時に携帯電話機に対して付加価値情報をダウンロードする機能を有している。利用者情報データベース１は電子商取引を行う携帯電話機２の電話番号と、そこにセットされるＳＩＭカードの識別情報（例えばＩＤ番号）が事前に登録されている。

【０００７】電子商取引に際し、携帯電話機２からホストサーバー３へアクセスすると、ＳＩＭカード４のＩＤ番号が携帯電話番号とともにホストサーバー３へ通知される。ホストサーバー３はＳＩＭカードのＩＤ番号と使用中の携帯電話番号の組み合わせについて利用者情報データベース１を参照して照合する。ＳＩＭカードのＩＤ番号と携帯電話番号の組み合わせが利用者情報データベース１に事前登録された内容と一致する場合のみ、ホストサーバー３は付加価値情報のダウンロード等のサービスを提供する。もし、不一致の場合は、サービス要求は受け付けない。これにより、ＳＩＭカードの盗難、紛失の場合に自分以外の携帯電話機からの利用ができなくなり、不正なモバイル電子商取引を防ぐことができる。

【０００８】本発明のシステムにおけるサービスは、例えば電子マネー、交通チケット、イベントチケットなどの付加価値情報をＳＩＭカードにダウンロードして実際の店舗で使用する場合に適用可能である。

【０００９】

【発明の効果】以上のように、本発明によれば、携帯電話番号とカード識別情報とを事前に登録しておき、電子商取引に際しては、携帯電話番号とカード識別情報とを照合して事前登録した内容と一致する場合のみサービスを提供するようにしたので、カードの盗難や紛失時における不正なモバイル電子商取引を防ぐことができ、セキュリティを確保して電子商取引環境の向上を図ること可能となる。

【図面の簡単な説明】

【図１】　携帯電話による電子商取引システムを説明する概念図である。

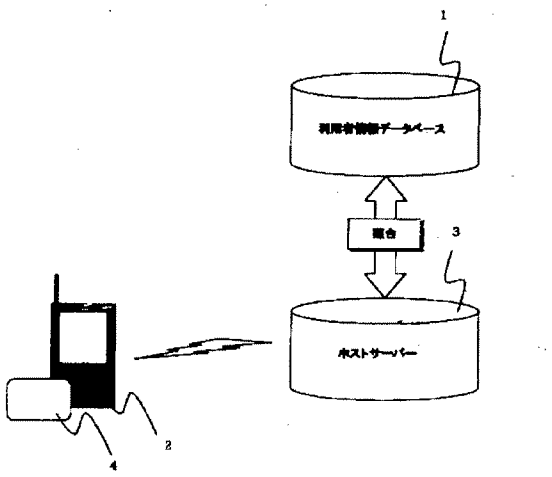
【符号の説明】

１…利用者情報データベース、２…携帯電話機、３…ホ

３

ストサーバー、４…ＳＩＭカード。

【図１】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
Ｇ０６Ｆ　17/60	５０６	Ｇ０６Ｆ　17/60	５０６
	５１０		５１０
Ｇ０６Ｋ　17/00	ＺＥＣ	Ｇ０６Ｋ　17/00	ＺＥＣＳ

(72)発明者　南部啓一
東京都港区芝浦３丁目８番10号　ジェイアール東日本メカトロニクス株式会社内

(72)発明者　佐藤正信
東京都港区芝浦３丁目８番10号　ジェイアール東日本メカトロニクス株式会社内

Ｆターム(参考)　5B058 CA27 KA02 KA04 KA31 YA02

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-338814
(43)Date of publication of application : 28.11.2003

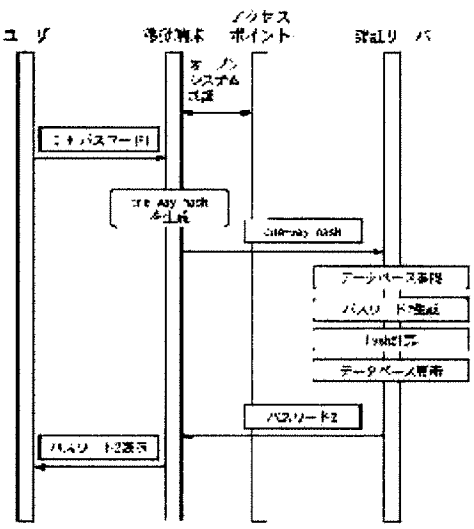
(51)Int.Cl. H04L 9/32
G06F 15/00
G06K 17/00
G06K 19/10
H04Q 7/38

(21)Application number : 2002-145201
(22)Date of filing : 20.05.2002

(71)Applicant : CANON INC
(72)Inventor : KANDA TETSUO

(54) COMMUNICATION SYSTEM, ADMINISTRATIVE SERVER, CONTROL METHOD THEREFOR AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a high-security communication system in which a generated one-time password is surely delivered and illegal access from a third person is effectively blocked.
SOLUTION: In a management method for the communication system including a radio terminal on a wireless network and a server device for controlling access from the radio terminal to a wired network on the relevant wired network, an authentication procedure is implemented between the radio terminal and the server device and when first authentication information obtained from the radio terminal is authenticated by the server device in the authentication procedure, second authentication information in place of the first authentication information is generated. Then, the second authentication information is transmitted to the radio terminal while being contained in an authentication permission message as authentication information which can be authenticated by the radio terminal in the next authentication procedure.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－338814
（P2003－338814A）
(43)公開日　平成15年11月28日(2003.11.28)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	9/32		Ｇ０６Ｆ	15/00	３３０Ｃ　５Ｂ０３５
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｋ	17/00	Ｔ　５Ｂ０５８
Ｇ０６Ｋ	17/00		Ｈ０４Ｌ	9/00	６７３Ｄ　５Ｂ０８５
	19/10		Ｇ０６Ｋ	19/00	Ｒ　５Ｊ１０４
Ｈ０４Ｑ	7/38		Ｈ０４Ｂ	7/26	１０９Ｓ　５Ｋ０６７

審査請求　未請求　請求項の数９　ＯＬ　（全 15 頁）

(21)出願番号　特願2002－145201(P2002－145201)

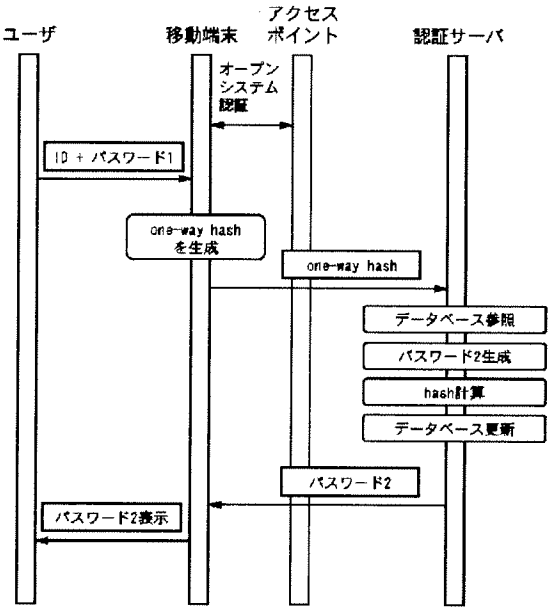
(22)出願日　平成14年５月20日(2002.5.20)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　神田　哲夫
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100076428
弁理士　大塚　康徳　（外３名）

最終頁に続く

(54)【発明の名称】　通信システム、管理サーバおよびその制御方法ならびにプログラム

(57)【要約】
【課題】　生成したワンタイム・パスワードを確実に配送することができ、第三者からの不正アクセスを有効に防御できる安全性の高い通信システムを提供すること。
【解決手段】　無線ネットワークにおける無線端末と、有線ネットワークにおいて前記無線端末の当該有線ネットワークへのアクセスを制御するサーバ装置とを含む通信システムの管理方法であって、前記無線端末と前記サーバ装置との間で認証手順を実行し、その認証手順において、前記無線端末から得られた第１の認証情報が前記サーバ装置によって認証されたとき、第１の認証情報にかわる第２の認証情報を生成し、その第２の認証情報を前記無線端末が次回の認証手順において認証可能な認証情報として認証許可メッセージに含めて前記無線端末に送信する。



1

【特許請求の範囲】

【請求項１】　無線ネットワークにおける無線端末と、有線ネットワークにおいて前記無線端末の当該有線ネットワークへのアクセスを制御するサーバ装置とを含む通信システムであって、

前記無線端末と前記サーバ装置との間で認証手順を実行する認証手段と、

前記認証手順において前記無線端末より得られた第１の認証情報が前記サーバ装置によって認証されたとき、第１の認証情報にかわる第２の認証情報を、前記無線端末が次回の認証手順において認証可能な認証情報として認証許可メッセージに含めて前記無線端末に送信する送信手段と、

を備えることを特徴とする通信システム。

【請求項２】　前記無線端末は、受信した前記認証許可メッセージに含まれる前記第２の認証情報を表示する表示手段を備えることを特徴とする請求項１に記載の通信システム。

【請求項３】　前記無線端末は、

メモリカードを装着するためのスロットと、

前記第１の認証情報が記録されたメモリカードを前記スロットに装着することでその第１の認証情報を取得する取得手段と、

受信した前記認証許可メッセージに含まれる前記第２の認証情報でもって前記メモリカードに記録されている前記第１の認証情報を書き換える書き換え手段と、を備えることを特徴とする請求項１に記載の通信システム。

【請求項４】　本通信システムは、コネクションの確立手順を経ずに通信を行うコネクションレス型の通信システムであることを特徴とする請求項１から３までのいずれかに記載の通信システム。

【請求項５】　無線ネットワークにおける無線端末と、有線ネットワークにおいて前記無線端末の当該有線ネットワークへのアクセスを制御するサーバ装置とを含む通信システムを管理する方法であって、

前記無線端末と前記サーバ装置との間で認証手順を実行する認証ステップと、前記認証ステップで、前記無線端末から得られた第１の認証情報が前記サーバ装置によって認証されたとき、第１の認証情報にかわる第２の認証情報を、前記無線端末が次回の認証手順において認証可能な認証情報として認証許可メッセージに含めて前記無線端末に送信する送信ステップと、

を有することを特徴とする方法。

【請求項６】　無線ネットワークおよび有線ネットワークを含む通信システムにおいて前記有線ネットワークにアクセスしようとする無線端末の当該アクセスを管理する管理サーバであって、

前記有線ネットワークへの参加を許可しうる認証情報を登録した登録リストと、

前記無線端末より受信した認証要求メッセージから得られる第１の認証情報が前記登録リストに含まれているか否かによって認証を行う認証手段と、

前記認証が成功したときに、前記無線端末の次回の認証時に認証可能な認証情報としての第２の認証情報を生成する生成手段と、

生成した前記第２の認証情報でもって前記登録リスト中の前記第１の認証情報を更新する更新手段と、

生成した前記第２の認証情報を認証許可メッセージに含めて前記無線端末に送信する送信手段と、

を備えることを特徴とする管理サーバ。

【請求項７】　前記通信システムは、コネクションの確立手順を経ずに通信を行うコネクションレス型の通信システムであることを特徴とする請求項６に記載の管理サーバ。

【請求項８】　無線ネットワークおよび有線ネットワークを含む通信システムにおいて前記有線ネットワークにアクセスしようとする無線端末の当該アクセスを管理する管理サーバの制御方法であって、

前記有線ネットワークへの参加を許可しうる認証情報を登録した登録リストをあらかじめ記憶しておき、

前記無線端末より受信した認証要求メッセージから得られる第１の認証情報が前記登録リストに含まれているか否かによって認証を行う認証ステップと、

前記認証が成功したときに、前記無線端末の次回の認証時に認証可能な認証情報としての第２の認証情報を生成する生成ステップと、

生成した前記第２の認証情報でもって前記登録リスト中の前記第１の認証情報を更新する更新ステップと、

生成した前記第２の認証情報を認証許可メッセージに含めて前記無線端末に送信する送信ステップと、

を有することを特徴とする管理サーバの制御方法。

【請求項９】　無線ネットワークおよび有線ネットワークを含む通信システムにおいて前記有線ネットワークにアクセスしようとする無線端末の当該アクセスを管理する管理サーバの制御用プログラムであって、

前記有線ネットワークへの参加を許可しうる認証情報をあらかじめ登録して記憶しておいた登録リストに、前記無線端末より受信した認証要求メッセージから得られる第１の認証情報が含まれているか否かによって認証を行う認証ステップ、

前記認証が成功したときに、前記無線端末の次回の認証時に認証可能な認証情報としての第２の認証情報を生成する生成ステップ、

生成した前記第２の認証情報でもって前記登録リスト中の前記第１の認証情報を更新する更新ステップ、

生成した前記第２の認証情報を認証許可メッセージに含めて前記無線端末に送信する送信ステップ、

を実行させるプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は通信システムに関し、特に、無線通信端末が無線ネットワークを介して有線ネットワークに参加するときの認証技術に関する。

【０００２】

【従来の技術】無線ＬＡＮシステムは従来より、通信ケーブルに拘束されない可搬性の優れたネットワークシステムとして利用されており、近年は特に、無線通信区間の伝送速度の向上や、ノート型パソコンの普及、モバイル通信に適したアプリケーションの出現などにより、飛躍的な普及を見せている。とりわけ2.4GHzや5GHz帯の電波を用いた無線ＬＡＮシステムとして、IEEE802.11規格群によって規定された無線ＬＡＮシステムが一般的に普及している。

【０００３】しかしながら、このような無線ＬＡＮシステムは高い利便性の反面、電波を用いたワイヤレス通信方式であるため、通信における秘匿性や信頼性の低さが指摘されてきた。

【０００４】たとえば、電波はその性質上、いったん送信機から空間中に送出されると、宛先となるべき移動端末以外の第三者が傍受することが可能であり、情報としての通信データが外部の第三者に対して漏洩するおそれがある。また、無線ＬＡＮシステムは、有線のＬＡＮがケーブルによって物理的に接続される運用形態ではなく、一般に移動端末の通信を管理する基地局に対しての無線通信手順によって論理的に接続される。したがって、自組織外の第三者の移動端末が過誤により、あるいは故意にネットワークに接続される事態が生じるおそれがある。

【０００５】このような問題を防ぐために、無線ＬＡＮシステムでは、上位のアプリケーション層から下位のＭＡＣ（Media Access Control）層、あるいは物理層までの各層において、各種の方式によって対策を行っている。とくに無線信号の傍受による情報の漏洩に対してはデータの暗号化などによって対応し、外部からの不正な接続に対しては認証方式を採用することによりこれらの問題を回避することが一般的である。具体的にはデータの暗号化方式としては、IEEE802.11規格によってＷＥＰ（Wire Equivalent Privacy）アルゴリズムを用いた共通秘密鍵方式が規定されており、一方、認証方式としては無線ＬＡＮアクセスポイントの多くが、自組織に用いられる移動端末のＭＡＣアドレスを登録することによって、自組織外の第三者からのアクセスを防禦する方式がとられている。

【０００６】さらに安全性を高めるべく、認証キーとして使用するパスワードを逐次変更していき、万が一パスワードが第三者に漏洩しても、新規に更新されたパスワードを用いることでそれ以降の不正アクセスを防ぐ方法が考えられている。かかる方法はいわゆるワンタイム・パスワード方式として知られている。このようなワンタイム・パスワード方式を携帯電話に応用した従来技術と

して特開平5-336109号が挙げられる。これによれば、電話での通話が終了する時に新たに乱数を発生し、この乱数を次回の発呼時に認証キーとして利用する。つまり、新たな認証キーはコネクションの終了フェーズにおいて携帯電話に配送される。

【０００７】

【発明が解決しようとする課題】しかしながら、このワンタイム・パスワード方式は、携帯電話のように接続と終話処理が明確であるコネクション型の通信システムには比較的適用しやすいものの、無線ＬＡＮのようなコネクションレス型の通信システムには適用が容易でないという問題がある。

【０００８】具体的には、ＬＡＮの運用形態では、例えばサーバへのアクセスの開始に際してセッションのログイン処理が行われるが、セッションの終了に際して必ずしも明確なログオフ処理をすることは一般的に少なく、ユーザは端末利用が終わるとサーバへの接続開放などの手続きを行わず、端末の電源を切ってしまう場合が多い。さらに、ＬＡＮは携帯電話のような通信システムよりもネットワークとしての接続性は低く、ネットワークの障害や、あるいは端末機器、サーバなどの停止によって、通信が強制的に終了してしまう事態も多く発生する。携帯電話システムがユーザの終話時に、コネクションの終了フェーズとして通信チャネルの開放や課金情報の取り込みなど多くの処理を行うことに比べて、無線ＬＡＮではセッションの終了が明確ではない。したがって、上記の携帯電話システムの如くコネクションの終了フェーズにおいて新たなパスワードを配送する方式をそのまま無線ＬＡＮに適用する場合には、新たなパスワードを確実に配送することが保証されないことになる。

【０００９】そこで、本発明は、生成したワンタイム・パスワードを確実に配送することができ、第三者からの不正アクセスを有効に防御できる安全性の高い通信システムを提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明の第１の側面は、無線ネットワークにおける無線端末と、有線ネットワークにおいて前記無線端末の当該有線ネットワークへのアクセスを制御するサーバ装置とを含む通信システムおよびその管理方法に関する。この第１の側面によれば、本通信システムは、前記無線端末と前記サーバ装置との間で認証手順を実行し、前記認証手順において前記無線端末より得られた第１の認証情報が前記サーバ装置によって認証されたとき、第１の認証情報にかわる第２の認証情報を、前記無線端末が次回の認証手順において認証可能な認証情報として認証許可メッセージに含めて前記無線端末に送信する。

【００１１】本発明の第２の側面は、無線ネットワークおよび有線ネットワークを含む通信システムにおいて前記有線ネットワークにアクセスしようとする無線端末の

当該アクセスを管理する管理サーバおよびその制御方法に関する。この第２の側面によれば、前記管理サーバは、前記有線ネットワークへの参加を許可しうる認証情報を登録した登録リストを有しており、前記無線端末より受信した認証要求メッセージから得られる第１の認証情報が前記登録リストに含まれているか否かによって認証を行い、前記認証が成功したときに、前記無線端末の次回の認証時に認証可能な認証情報としての第２の認証情報を生成し、生成した前記第２の認証情報でもって前記登録リスト中の前記第１の認証情報を更新し、そして、生成した前記第２の認証情報を認証許可メッセージに含めて前記無線端末に送信する。また、この制御方法による一連の処理は、プログラムによっても実現されうる。

【００１２】

【発明の実施の形態】本発明の利点を説明する前に、認証技術に関する予備的事項を追加的に説明しておく。

【００１３】まず、IEEE802.11規格によって規定されたＷＥＰアルゴリズムを用いた共通鍵認証方式について説明する。

【００１４】図６は一般的な無線ＬＡＮシステムの構成を示した図である。無線ＬＡＮステーション（ＳＴＡ）２１は、図示のように移動端末２１１に無線ＬＡＮカード２１２が装着された構成である。IEEE802.11規格では、アクセス方式としてアドホックモード、およびインフラストラクチャモードの２種類が定義されており、通常一時的な無線通信、例えばＳＴＡとＳＴＡの一対一通信のような簡単なトポロジー構成ではアドホックモードが用いられ、一方、多数の移動端末がアクセスする大きなネットワーク構成ではインフラストラクチャモードが用いられる。インフラストラクチャモードでは、基地局として図中に示したアクセスポイント（ＡＰ）２２が移動端末の制御をつかさどる。さらに、アクセスポイントは有線ネットワーク２３に接続され、移動端末との無線区間での通信と有線基幹ネットワークでの通信の橋渡しもする。

【００１５】IEEE802.11による認証方式としては、鍵を用いないオープンシステム認証方式と、ＳＴＡが同一の共通秘密鍵を持つ共通鍵認証方式の２種類が規定されている。このうち図７はＷＥＰアルゴリズムによる共通鍵認証方式による動作を示したシーケンス図である。この認証処理は、例えば２個のＳＴＡのみから構成されるアドホックモードにおいてはＳＴＡ間で行われ、アクセスポイントを介したインフラストラクチャモードにおいては、ＳＴＡからアクセスポイントへの認証動作となる。本図はインフラストラクチャモードにおけるＳＴＡからＡＰへの認証動作を表している。

【００１６】まず、本図において認証要求を求める移動端末（ＳＴＡ）はアクセスポイントに対して認証要求のための第１のマネジメントパケット（Ｐ１）を送出する。このＰ１は移動端末に装着された無線ＬＡＮカードのＭＡＣアドレスを保持し、平文にて伝送される。アクセスポイントはＰ１を受け取ると、アクセスポイントに具備された乱数発生器によりランダムな128バイトのデータを生成し、このランダムデータを第２のマネジメントパケット（Ｐ２）として、認証要求を行ったＳＴＡに対して返送する。ここで、このＳ２はチャレンジテキストと呼ばれる。

【００１７】次に、このチャレンジテキストを受信した移動端末はＷＥＰを起動する。図８はＷＥＰアルゴリズムによる暗号化ブロックの構成図である。ここで、ＷＥＰアルゴリズムで使用される暗号化キーは、共通鍵部分（Shared Key）とイニシャライゼイション・ベクタ（IV）から構成される。共通鍵は一般にESSIDと呼ばれ、あらかじめ管理者によってすべての移動端末とアクセスポイントに同一の鍵が設定されている。一方、イニシャライゼイション・ベクタは暗号化を行うＳＴＡが任意に生成するキーであり、パケット伝送ごとにパケットに添付されて相手先に伝えられる。

【００１８】ここで、暗号化を行う移動端末はイニシャライゼイション・ベクタとして24ビットの任意の値を決定する。移動端末はこのイニシャライゼイション・ベクタと40ビットの共通秘密鍵を連結した64ビット値を乱数発生器に乱数シードとして与える。乱数発生器はこの乱数シードから暗号キーストリームとしての乱数系列（Key Sequence）を生成し、伝送される平文データ（Plain Text）とこの乱数系列との排他的論理和演算によって暗号化テキスト（Cipher Text）が生成される。また同時にデータの完全性を確認するために、CRC-32によるインテグリティ・アルゴリズムによって一種のチェックサムとして32ビットのICVが生成される。このようにして作られた暗号化テキスト、IV、ICVはすべてパケット伝送によって相手先に伝えられる。

【００１９】このＷＥＰアルゴリズムはデータパケットの暗号化に使用されるが、いま説明している認証シーケンスにおいては、ＳＴＡはこのＷＥＰアルゴリズムにより、ＡＰから受け取ったチャレンジ・テキストを暗号化する。図７のシーケンスにおいて、ＳＴＡは受信したチャレンジテキスト（Ｐ２）に対して、これを暗号化したデータパケット（Ｐ３）をアクセスポイントに対して送信する。ここで、Ｓ３はＷＥＰアルゴリズムによって生成された暗号化パケットであり、暗号化テキストと共に暗号化に用いられたIV、さらにデータ整合性の確認のためのICVが添付されてＡＰに伝えられる。

【００２０】アクセスポイントは内部に実装されたＷＥＰ復号化ブロックによってこのＰ３パケットの検査と解読を行う。アクセスポイントは図９に示すＷＥＰ復号化ブロックにて、あらかじめ設定された40ビットの共通秘密鍵、および受信したパケットＰ３に含まれるIVから、暗号化ブロックと同様に64ビットの乱数シードを生成

し、この乱数シードから乱数発生器が乱数系列を生成する。共通秘密鍵、およびIVはＳＴＡで暗号化された時に使われたものと同一であるので、ここで作られる乱数系列はＳＴＡで暗号化されたときの系列と同じになり、結果としてアクセスポイントはＳＴＡによって暗号化されたチャレンジ・テキストを解読することができる。

【００２１】アクセスポイントは復号した平文から、まずインテグリティ・アルゴリズム検査部で受信した平文のICVを計算し、受信パケットに記録されているICVとの比較を行う。これが同一であれば、次に復号化した平文がＰ２において自分からＳＴＡに対して送出したチャレンジテキストと同一であるかを比較する。この結果、チャレンジテキストが同じであれば、アクセスポイントは当該ＳＴＡが同一の共通鍵を持つ相手だと認識し、認証が成功する。アクセスポイントはこの認証結果を第４のマネジメントパケット（Ｐ４）によってＳＴＡに通知し、認証処理が完了する。

【００２２】以上、述べてきたのはIEEE802.11規格によって規定されている無線ＬＡＮの認証方式である。しかしながら、このようなＷＥＰアルゴリズムによる認証方式だけでは、無線ネットワークの十分な安全性は確保できないと考えられる。なぜなら、ＷＥＰアルゴリズムではアクセスポイント、および移動端末が共通に保持する共通鍵を確認することで認証を行っているだけであり、この鍵を知りえた外部の第三者は、自分の移動端末にこの共通鍵を設定することで容易に当該無線ネットワークへアクセスすることが可能となるからである。特に、この共通鍵の設定は例えばコンピュータシステム上で利用者が手入力で行うことができるため、利用者にとって比較的容易な手段で不正アクセスすることが可能である。さらに、多数の移動端末が同一の共通鍵を使用するような本システムでは、共通鍵が外部に知られてしまう危険性は大きく、意図的な悪意の第三者による不正アクセスに対しては十分に安全な防御方法とはならないといえる。

【００２３】そのため一般の無線ＬＡＮシステムでは、IEEE802.11規格によるＷＥＰアルゴリズム認証以外にも、ＭＡＣアドレス登録機能を利用した認証方式を併用している。これは、あらかじめすべての移動端末に装着された無線ＬＡＮカードの持つ６バイトのＭＡＣアドレスを、アクセスポイントに実装されたＭＡＣアドレス管理データベースに登録する方法である。無線区間を伝送するすべてのマネジメントフレーム、データフレームには、そのパケットを送出した発信元のＭＡＣアドレスが記録されているため、アクセスポイントはそのＭＡＣアドレスを確認することによって自組織内の正当な移動端末からのアクセスであるかどうか判断することができる。例えば図７に示した認証シーケンスにおいて、第１のマネジメントパケット（Ｐ１）には認証要求をしている移動端末のＭＡＣアドレスが記録されている。したがって、アクセスポイントは本認証要求パケットのＭＡＣアドレスが、自分の持つＭＡＣ管理用データベースに登録されているかどうかの検索を行い、もしも未登録のアドレスであれば認証シーケンスの過程で認証処理を不成功にすることができる。

【００２４】このようなＭＡＣアドレス登録方式の利点は、ＭＡＣアドレスが無線ＬＡＮカードの製造時にそれぞれのカードにユニークに実装されるアドレスであり、仮に第三者が無線ネットワーク上のアクセスポイントに登録されているＭＡＣアドレスのひとつを知りえたとしても、ＭＡＣアドレスの書き換えには無線ＬＡＮカードに実装されている不揮発性メモリなどの該当するアドレスの内容を書き換えるような操作が必要であり、前述のＷＥＰ共通鍵の設定と比較すると困難な作業となる。また、自分がなりすましたＭＡＣアドレスを持つ正当な無線ＬＡＮカードが同時に稼動している場合には、マネジメントフレーム、データフレームの流れの不一致性などから、アクセスポイントによって不正アクセスを検出されやすく、ＷＥＰアルゴリズムのみの認証方式と比較すると、より安全性の高いシステムといえる。

【００２５】しかしながら、このようなアクセスポイントによるＭＡＣアドレスを管理する方法の欠点としては、当該無線ネットワークに参加すべき移動端末すべてのＭＡＣアドレスをアクセスポイントに登録しなければならない点が挙げられる。特にアクセスポイントが複数個存在する場合には、すべてのアクセスポイントに対して、このＭＡＣアドレス登録の作業が必要となり、ネットワーク管理のための工数が飛躍的に増大する。仮にアクセスポイントが数十台、数百台もあるような大規模な組織であれば、すべてのアクセスポイントへのＭＡＣアドレス登録を正しく保守、管理する作業は現実的と言えない。

【００２６】したがって大規模なネットワークにおいてＭＡＣアドレスによる認証方式を利用するためには、ＭＡＣアドレスをアクセスポイントに登録するのではなく、アクセスポイントの他に認証処理を制御する単一のサーバを準備し、この認証サーバのみにＭＡＣアドレスを登録することによって少ない工数でネットワーク全体の安全性を管理できるようにする技術もある。このような従来技術としては、例えば特開2001-111544号に記されているようなものがあげられる。図１０はこの従来技術による無線ＬＡＮシステムの構成を示した図である。図中、有線ネットワーク２３には認証サーバ２５が接続されていることが特徴である。この従来例では認証方式としてＲＡＤＩＵＳ（Remote Authentication Dial In User Service）方式を利用しており、認証サーバはＲＡＤＩＵＳサーバとして移動端末のＭＡＣアドレスを登録された管理用データベースを具備している。一方、アクセスポイントにはＭＡＣアドレスのデータベースを持っておらず、ＲＡＤＩＵＳクライアントとして動作する。

【００２７】図１１は一般的な認証処理を示したシーケンス図である。まず、無線ネットワークに参加しようとする移動端末は、アクセスポイントに対して認証要求を送出する。この認証要求パケットには当該移動端末のＭＡＣアドレスが記録されている。要求を受けたアクセスポイントは、通常のＷＥＰアルゴリズムではチャレンジテキストを移動端末に返送するが、ここではアクセスポイントから認証サーバに対して、移動端末のＭＡＣアドレスを認証のＩＤとして送出する。ここで、認証サーバはＲＡＤＩＵＳプロトコルによってアクセスポイントから受け取った移動端末のＭＡＣアドレスを認証する。次に認証に成功した認証サーバは、アクセスポイントに対してチャレンジテキストを送出する。認証サーバからチャレンジテキストを受け取ったアクセスポイントは本来のＷＥＰアルゴリズムに戻って、移動端末に対するチャレンジテキストを移動端末へ送信する。

【００２８】以後、通常のＷＥＰアルゴリズムにしたがって、移動端末はアクセスポイントから受信したチャレンジテキストに対し、共通鍵とIVにより暗号化を行う。この暗号文とIVは移動端末からアクセスポイントへ送信され、アクセスポイントはこの暗号文を解読し、ICVなどのチェックを経て認証を行う。そして、認証に成功したアクセスポイントは認証サーバにレスポンスを返す。

【００２９】上述の図１１に示したようなネットワーク構成では、認証処理に利用するＭＡＣアドレスのデータベースは認証サーバにて一元的に管理されているため、管理者はこのデータベースのみを更新することによって当該ネットワークに含まれる移動端末のＭＡＣアドレスを完全に管理することができるようになり、すべてのアクセスポイントにＭＡＣアドレスを登録する場合と比較し簡便にネットワークを管理することが可能となる。このようにして、IEEE802.11規格に規定されたＷＥＰアルゴリズムに、さらに認証サーバによる移動端末のＭＡＣアドレス管理方式を追加することによって、より高度な認証を行っている。

【００３０】上記のとおり、ＭＡＣアドレスによる認証方式を追加することで、IEEE802.11規格に規定されたＷＥＰアルゴリズムのみの認証方式よりも安全性が高められ、またＭＡＣアドレスの管理を認証サーバで一元的に行うことで保守作業の簡易化も図れることがわかる。

【００３１】しかしながら、これまで説明してきた各方式では、認証のキーとして用いているＷＥＰ共通鍵やＭＡＣアドレスなどの情報は、すべて機器としての無線ＬＡＮカード、あるいはそれが装着されている移動端末に割り振られているものであり、実際の使用者に対しての認証が行われているわけではない。これらの認証処理は、正当な機器は正当な利用者によって利用されているという前提によってなされているものであり、例えば紛失や盗難によって無線ＬＡＮカード自体を入手した外部の第三者にとっては、本認証システムにおいてネットワークにアクセスすることは可能である。あるいは、非常に巨大な組織では、ある移動端末は複数の利用者によって使用されたり、逆に一人の利用者が複数の移動端末を利用することも多く、このような流動的な組織では頻繁に新たな無線端末が導入されたり、廃棄されたりなどするため、ＭＡＣアドレスによる機器レベルの管理では、不具合が生じることも多い。

【００３２】さらに、「なりすまし」のために自らの移動端末のＭＡＣアドレスを書き換える作業をいとわない悪意の第三者に対しては、ＭＡＣアドレス管理による認証方式でさえ十分な認証方法とは言えない。当該ネットワークに参加を許された移動端末のＭＡＣアドレスを知り得た悪意の第三者は、自分の移動端末から当該ＭＡＣアドレスを用いることにより、正当な端末になりすますことが可能である。この場合、さらに悪いことにＭＡＣアドレスはそれぞれの移動端末に装着された無線ＬＡＮモジュールに製造時に割り振られた数字であり、利用者はこれを自由に変更することはできないため、いったん自組織のＭＡＣアドレスが外部に漏れた場合には、正当な利用者はこのＭＡＣアドレスを持った無線ＬＡＮカードを使い続けることができなくなる。このような事態は、認証方式に用いるキーとして、永久に固定値となるＭＡＣアドレスのようなデータを用いていることに起因する。すなわち、通信ネットワークにおいて、十分に安全で管理の容易な認証方式として使用する認証キーとしては、すべての移動端末とアクセスポイントが共通の鍵を持つ方式よりも、移動端末あるいは利用者が個々に設定できる認証キーが有効であり、さらに万が一、その認証キーが外部に漏れた際には、遅滞なく新しい認証キーに変更できるような柔軟な方式が望ましいといえる。

【００３３】また、これまで挙げてきた例による認証方式では、ネットワークを利用するユーザに対して認証を行っているわけでなく、ESSIDを登録された移動端末、あるいはＭＡＣアドレスを持った無線ＬＡＮカードなど、通信機器に対しての認証を行う方式であった。ネットワークに対して実際に不正アクセスを試みるのは利用者であり、無線ＬＡＮシステムのみならず一般に通信ネットワークにおいて高度な安全性を必要とする場合、ＭＡＣアドレス管理のような機器に対する認証方式ではなく、利用者個人を正当なユーザであるか外部の第三者であるかを特定できるような認証方式が必要となる。

【００３４】図１２は、利用者を認証するシステムの例として、ＲＡＤＩＵＳ認証サーバを用いてユーザレベルでの認証システムを構築したネットワーク構成を示す図である。この例において、認証サーバ２５に登録されている認証キーは無線ＬＡＮカードのＭＡＣアドレスではなく、利用者３１－ａ～ｃそれぞれのユーザＩＤと個々のパスワードである。ユーザＩＤは複数の利用者を識別するために用いられる個々にユニークな文字列であり、これらの値は組織内部、あるいは組織外部に対して公開

されていても何ら問題はない。一方、パスワードについては、一般にユーザ３１－ａ～ｃはそれぞれ自分しか知らない文字列を決定し、あらかじめ認証サーバに登録しておく。

【００３５】図１３は本システムのおけるユーザ認証の手順を示したシーケンス図である。すべての利用者３１はそれぞれ固有のユーザＩＤを持ち、それぞれ自分しか知りえないパスワードを持つ。そして認証サーバに具備された認証用データベースには、これらユーザＩＤとパスワードがすべてあらかじめ登録されているものとする。

【００３６】図１３において、ネットワークにアクセスしたいユーザは、移動端末に自分のユーザＩＤとパスワードを入力する。移動端末とアクセスポイントはIEEE802.11規格に定められたオープンシステム認証によって認証が済んでおり、移動端末はアクセスポイントに対して下位層でのアクセスは可能である。ここで、移動端末はＲＡＤＩＵＳクライアントとして、ユーザから入力されたＩＤとパスワードから、一方向ハッシュ（one-way hash）操作によりハッシュデータを生成する。移動端末はこのハッシュをアクセスポイントに対して送出し、アクセスポイントはこれを有線ネットワークを介して認証サーバに伝える。認証サーバはＲＡＤＩＵＳサーバとして働き、自分の持つ認証用データベースに登録されているすべてのユーザＩＤおよびパスワードから、移動端末と同じ一方向ハッシュ操作によりハッシュデータを生成しておき、移動端末から受信したハッシュと、データベース上のハッシュを比較する。この検索操作でデータベース上に当該ハッシュが存在すれば、受信したハッシュがあらかじめ登録されている正当な利用者からのものであることが識別できるため、認証が成功する。認証サーバはこの認証結果をアクセスポイントを通じて移動端末に伝え、その結果を表示された利用者は自分がネットワークにアクセスできることを知る。

【００３７】以上説明したような、単一の認証サーバによるユーザレベルでのＩＤとパスワードを管理する方式は、従来の無線ＬＡＮ認証方式としては非常に高度な安全性を持った方式といえる。

【００３８】そして、さらに安全性を高めるために、いわゆるワンタイム・パスワードを使用することが考えられる。携帯電話システムでは、コネクションの終了フェーズにおいてワンタイム・パスワードを配送することが便宜であると考えられる。しかし、従来の技術の項で述べたとおり、コネクションの終了フェーズにおいてワンタイム・パスワードを配送することを、セッションの終了が明確でないことが多い無線ＬＡＮのようなコネクションレス型の通信システムに適用すれば、ワンタイム・パスワードの確実な配送が保証され得ないことは明らかである。

【００３９】そこで、本件発明者は、生成したワンタイム・パスワードをセッション終了時に配送するのではなく、認証許可メッセージに含めて配送することを提案する。

【００４０】以下、本発明の好適な実施形態について詳細に説明する。

【００４１】実施形態における無線ＬＡＮシステムのネットワーク構成は図１２に示したとおりのものであり、無線端末としての移動端末１３と、有線ネットワーク２３に接続されたアクセスポイント（基地局）２２および認証サーバ２５とを含んでいる。移動端末１３とアクセスポイント２２とで無線ネットワークが構成され、このアクセスポイント２２が無線ネットワークと有線ネットワーク２３との中継を行う。また、この無線ＬＡＮシステムは、コネクションの確立手順を経ずに通信を行うコネクションレス型の通信システムである。

【００４２】図２は認証サーバ２５の内部構成例を示す図である。認証サーバ２５は、有線ＬＡＮトランシーバ２によって有線ネットワーク２３に接続され、アクセスポイント２２を介して移動端末１３との通信を行う。さらに、認証サーバ２５は認証用データベース１２１を記憶している。認証用データベース１２１には、ユーザ認証のための各ユーザ（３１－ａ～ｃ）のユーザＩＤと、それぞれのユーザに対して現在設定されているパスワード、およびこれらユーザＩＤとパスワードから計算された一方向ハッシュが登録されている。また、認証サーバ２５には入力手段としてのキーボード１２３と表示手段としてのディスプレイ１２２が設けられており、管理者はこれらを用いて認証データベース１２１の管理を行うことができる。

【００４３】図３は移動端末１３の構成例を示した図である。移動端末１３は無線ＬＡＮモジュール５を具備し、これに装着されたアンテナ１４によってアクセスポイント２２と無線通信を行い、アクセスポイント２２を介して認証サーバ２５と通信する。さらに、移動端末１３は入力手段としてのキーボード１３２および表示手段としてのディスプレイ１３１を具備する。

【００４４】図１は、実施形態における無線ＬＡＮシステムでの認証処理を示すシーケンス図である。移動端末１３を用いて有線ネットワーク２３に参加しようとするユーザは、まず移動端末１３のキーボード１３２から自分のユーザＩＤおよびパスワードを入力する。図１のシーケンス図に示したように、移動端末１３は入力されたユーザＩＤとパスワードから一方向ハッシュを生成する。ここで現在設定されているパスワードをパスワード１とする。あらかじめオープンシステム認証によってアクセスポイント２２に対して認証が取れている移動端末１３は、アクセスポイント２２へこの一方向ハッシュを接続要求パケットとして無線伝送する。本実施形態においてはアクセスポイント２２自体は認証機能を持っておらず、アクセスポイント２２は移動端末１３から受け取

った一方向ハッシュをそのまま有線ネットワーク２３を介して認証サーバ２５に中継する。

【００４５】移動端末１３からこの一方向ハッシュを受け取った認証サーバ２５は、自分の持つ認証用データベース１２１の登録内容を検索する。この結果、受け取ったハッシュと同一のハッシュが存在する場合、この認証要求は正当なユーザからのものであると判断し、認証が成功する。

【００４６】その後、認証サーバ２５は、このユーザ向けのワンタイム・パスワードとして新規パスワード（パスワード２）を生成する。認証サーバ２５はこのユーザＩＤと新たに生成したパスワード２を用いて一方向ハッシュを計算し、新規パスワードおよび新規ハッシュでもって認証用データベース１２１の当該ユーザ欄を更新する。そして、認証サーバ２５はこのパスワード２を認証許可メッセージである認証許可パケットに含めてアクセスポイント２２経由で移動端末１３に返送する。認証許可パケットを受け取った移動端末１３は図３に示したディスプレイ１３１にこのパスワード２を表示しユーザに伝える。ユーザは、表示されたパスワード２を記憶しておき、次回ログイン時にこのパスワード２を用いてログインすることができる。

【００４７】このように、上述の実施形態によれば、生成されたワンタイム・パスワードはセッション終了時に配送されるのではなく、認証許可メッセージに含められて配送される。したがって、特に、コネクションの確立手順を経ずに通信を行うコネクションレス型でセッションの終了が明確でない通信システムにおいても、ワンタイム・パスワードを確実に配送することができる。

【００４８】なお、上述した例の移動端末１３は、受け取ったワンタイム・パスワードをディスプレイ１３１に表示してユーザに通知する構成であったが、移動端末１３に内蔵されたメモリまたは着脱自在のメモリ等に書き込むようにしてもよい。以下、具体例を示す。

【００４９】図４は他の実施形態における移動端末１３の構成を示した図である。本図において、移動端末１３はカードスロット１３３を具備する。カードスロット１３３は、フラッシュメモリ等のチップを内蔵したいわゆるメモリカード（スマートカードとも称される）１５を着脱できる構造となっており、さらにメモリカード１５はこの移動端末１３によってその内容が書き換えられるものとする。このメモリカード１５は有線ネットワーク２３への参加を許可されているユーザに対してあらかじめ配布されており、その記録内容として、それぞれのユーザのユーザＩＤおよび初期パスワードが記録されている。

【００５０】図５は、図４の構成を有する移動端末１３に対する認証処理の一例を示すシーケンス図である。まず、移動端末１３を用いてネットワーク２３に参加しようとするユーザは、カードスロット１３３に自分のメモリカード１５を装着する。移動端末１３は、このメモリカード１５が装着されたことを検出すると、メモリカード１５に記録されているユーザＩＤおよび初期パスワード（パスワード１）を読み込む。そして移動端末１３は、これらユーザＩＤおよびパスワード１から一方向ハッシュを生成し、これをアクセスポイント２２へ接続要求パケットとして無線伝送する。そして、アクセスポイント２２は移動端末１３から受け取った一方向ハッシュを有線ネットワーク２３を介して認証サーバ２５に中継する。

【００５１】移動端末１３からこの一方向ハッシュを受け取った認証サーバ２５は、認証用データベース１２１の登録内容を検索する。この結果、受け取ったハッシュと同一のハッシュが存在した場合、この認証要求は正当なユーザからのものであると判断し、認証が成功する。その後、認証サーバ２５はこのユーザ向けの新規パスワード（パスワード２）を生成する。認証サーバ２５はこのユーザＩＤと新たに生成したパスワード２を用いて一方向ハッシュを計算し、新規パスワードおよび新規ハッシュでもって認証用データベース１２１の当該ユーザ欄を更新する。そして、認証サーバ２５はこのパスワード２を含んだ認証許可パケットをアクセスポイント２２経由で移動端末１３に返送する。認証許可パケットを受け取った移動端末１３は、この認証許可パケットからパスワード２を読み取り、メモリカード１５に記録されていたパスワード１をパスワード２に書き換える。このとき、同時にディスプレイ１３１に接続が許可された表示される。

【００５２】ユーザは移動端末１３の使用が終了した時には、このメモリカードを移動端末１３から抜き取り、これを管理することになる。このように、メモリカードによってパスワードを管理することにより、ユーザが毎回更新されるパスワード（ワンタイム・パスワード）をその都度記憶しておく必要がなくなるという利点がある。

【００５３】以上説明したように、本発明の実施形態によれば、無線ＬＡＮシステムにおいてワンタイム・パスワードを用いることにより、パスワードの盗難による第三者からの不正アクセスを防止することができる。ここで、パスワードの更新がログイン直後に行われるので、無線ＬＡＮのようなコネクションレス型の無線ネットワークのようにセッションの終了が明確でない運用形態においても、生成されたワンタイム・パスワードが確実に配送され、次回ログイン時に正しく接続することができる。

【００５４】このワンタイム・パスワードを用いた認証手順によれば、万が一、第三者による不正アクセスがあった場合、この第三者からの接続時に認証サーバでパスワードの更新が行われるため、正当なユーザによる次回ログイン時に、ユーザと認証サーバ間のパスワードが一

致しないため、それ以前に不正アクセスがあったことを検知することもできる。このように、無線ＬＡＮシステムに本発明を適用すれば、従来よりも不正アクセスに対する安全性を高めることができるようになる。

【００５５】なお、上述の実施形態では認証プロトコルとしてＲＡＤＩＵＳサーバシステムを例に用いたが、一般的にユーザ認証方式として利用できる他の認証プロトコルを用いることも可能である。

【００５６】

【他の実施形態】以上、本発明の実施形態を詳述したが、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタ等）から構成されるシステムに適用しても、１つの機器からなる装置（例えば、複写機、ファクシミリ装置等）に適用してもよい。

【００５７】なお、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムを、システムあるいは装置に直接あるいは遠隔から供給し、そのシステムあるいは装置のコンピュータがその供給されたプログラムを読み出して実行することによっても達成される場合を含む。

【００５８】したがって、本発明の機能処理をコンピュータで実現するために、そのコンピュータにインストールされるプログラムコード自体も本発明を実現するものである。つまり、本発明の特許請求の範囲には、本発明の機能処理を実現するためのコンピュータプログラム自体も含まれる。

【００５９】その場合、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等、プログラムの形態を問わない。

【００６０】プログラムを供給するための記憶媒体としては、例えば、フレキシブルディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ等）、光磁気ディスク、磁気テープ、メモリカード等がある。

【００６１】その他、プログラムの供給方法としては、インターネットを介して本発明のプログラムをファイル転送によって取得する態様も含まれる。

【００６２】また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等の記憶媒体に格納してユーザに配布し、所定の条件をクリアしたユーザに対し、インターネットを介して暗号化を解く鍵情報を取得させ、その鍵情報を使用することで暗号化されたプログラムを実行してコンピュータにインストールさせて実現することも可能である。

【００６３】また、コンピュータが、読み出したプログラムを実行することによって、前述した実施形態の機能が実現される他、そのプログラムの指示に基づき、コンピュータ上で稼働しているＯＳ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現され得る。

【００６４】さらに、記憶媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によっても前述した実施形態の機能が実現される。

【００６５】

【発明の効果】本発明によれば、生成したワンタイム・パスワードを確実に配送することができ、第三者からの不正アクセスを有効に防御できる安全性の高い通信システムを提供することができる。

【図面の簡単な説明】

【図１】実施形態における無線ＬＡＮシステムの認証処理のシーケンス図である。

【図２】実施形態における認証サーバの構成を示す図である。

【図３】実施形態における移動端末の構成を示す図である。

【図４】実施形態における別の例による移動端末の構成を示す図である。

【図５】図４の構成を有する移動端末に対する認証処理の一例を示すシーケンス図である。

【図６】従来の無線ＬＡＮシステムの構成を示す図である。

【図７】IEEE802.11に規定されているＷＥＰアルゴリズムのシーケンス図である。

【図８】ＷＥＰ暗号化ブロックの構成図である。

【図９】ＷＥＰ復号化ブロックの構成図である。

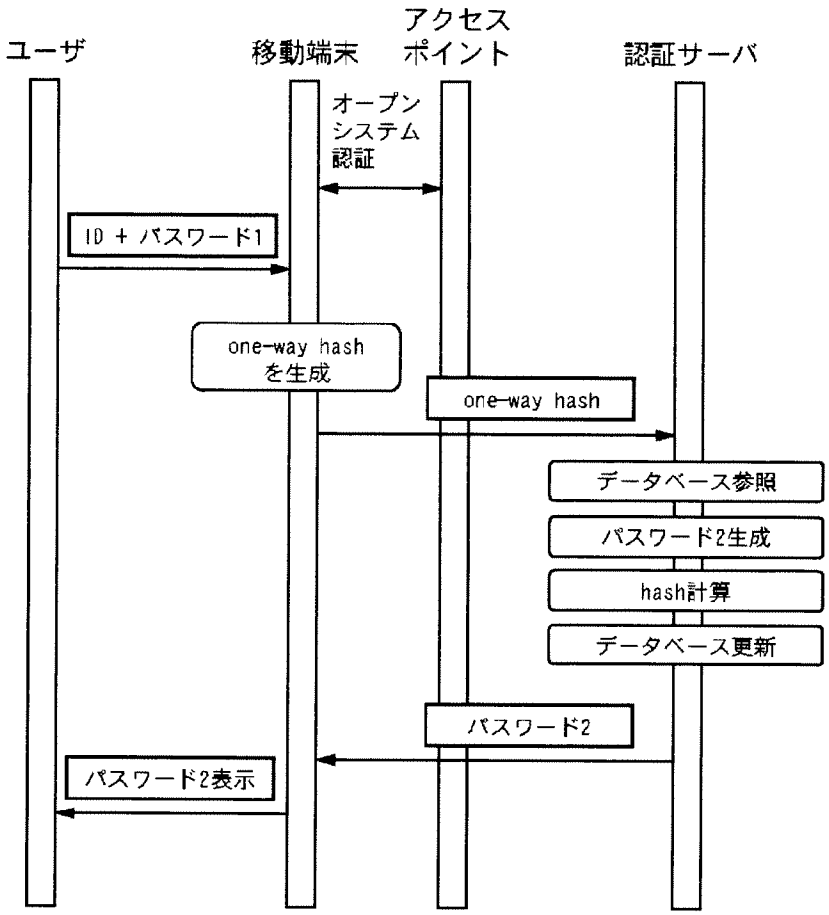
【図１０】従来の認証サーバを含む無線ＬＡＮシステムの構成を示す図である。

【図１１】従来の認証サーバによる認証処理のシーケンス図である。

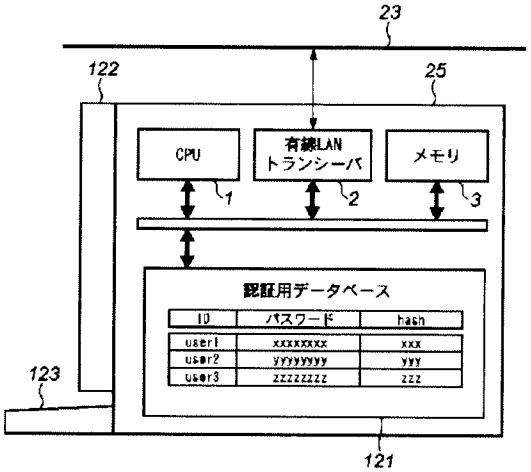
【図１２】実施形態におけるユーザ認証による無線ＬＡＮシステムの構成を示す図である。

【図１３】従来のユーザ認証による認証処理のシーケンス図である。

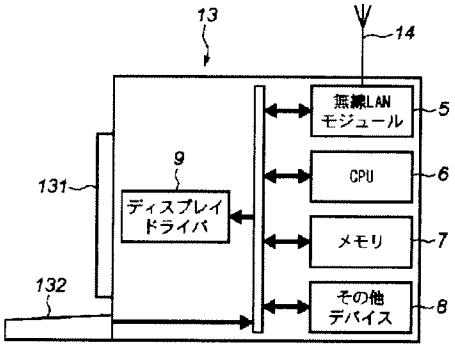
【図１】


ユーザ
移動端末
アクセス
ポイント
認証サーバ
オープン
システム
認証
ID + パスワード1
one-way hash
を生成
one-way hash
データベース参照
パスワード2生成
hash計算
データベース更新
パスワード2
パスワード2表示

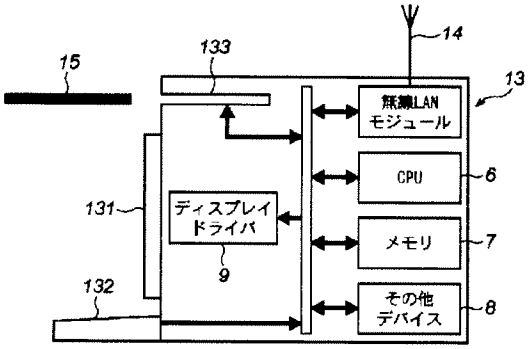
【図２】


23
122
25
CPU
有線LAN
トランシーバ
メモリ
1
2
3
認証用データベース
ID
パスワード
hash
user1
xxxxxxx
xxx
user2
yyyyyyy
yyy
user3
zzzzzzz
zzz
123
121

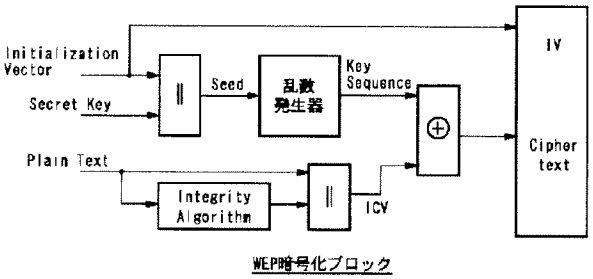
【図３】


13
14
無線LAN
モジュール
5
9
131
ディスプレイ
ドライバ
CPU
6
メモリ
7
132
その他
デバイス
8

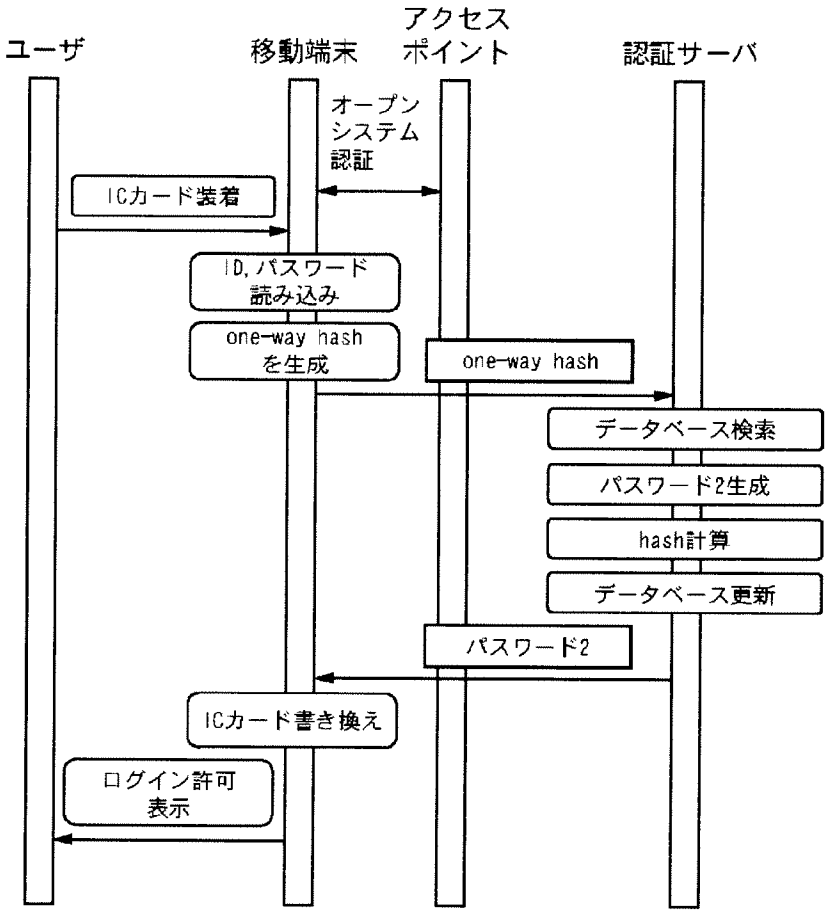
【図４】


15
133
14
13
無線LAN
モジュール
CPU
6
131
ディスプレイ
ドライバ
9
メモリ
7
132
その他
デバイス
8

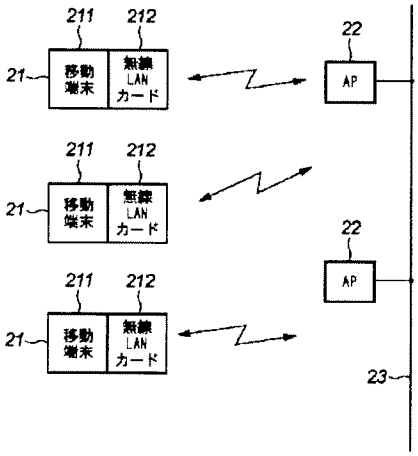
【図８】


Initialization
Vector
Secret Key
Seed
乱数
発生器
Key
Sequence
IV
Plain Text
Integrity
Algorithm
ICV
Cipher
text
WEP暗号化ブロック

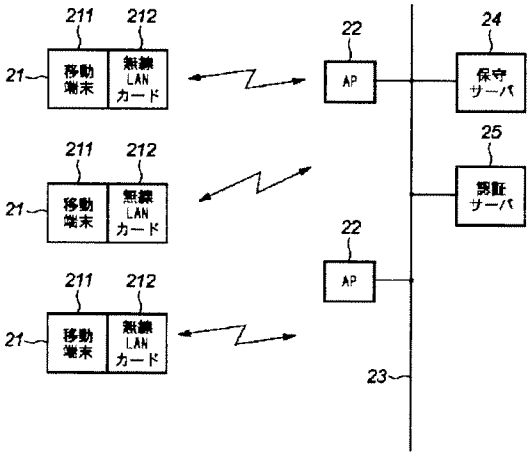
【図５】


ユーザ
移動端末
アクセス
ポイント
認証サーバ
オープン
システム
認証
ICカード装着
ID,パスワード
読み込み
one-way hash
を生成
one-way hash
データベース検索
パスワード2生成
hash計算
データベース更新
パスワード2
ICカード書き換え
ログイン許可
表示

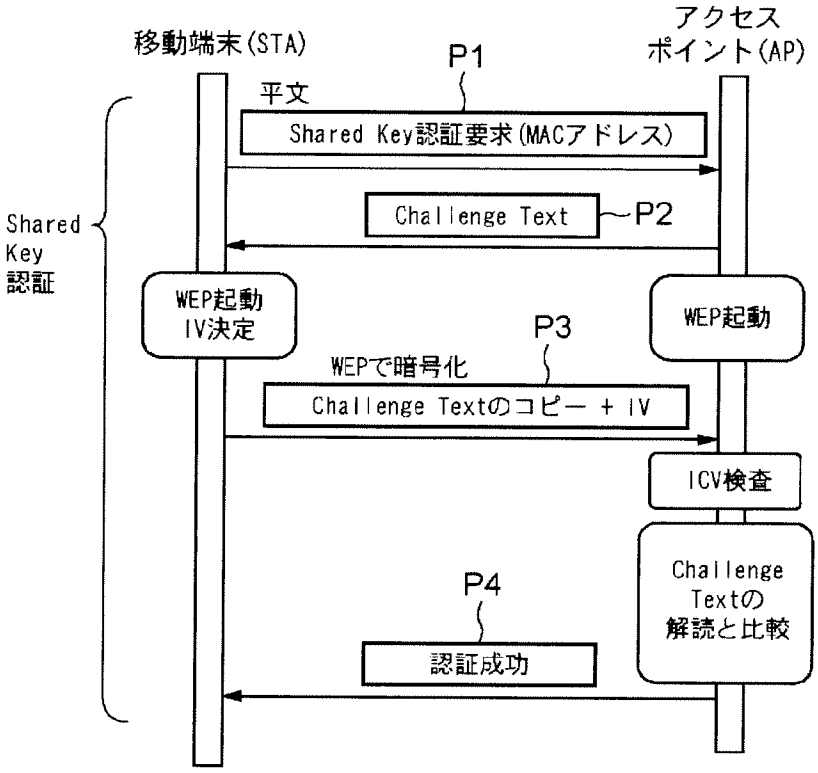
【図６】


211
212
21
移動端末
無線LANカード
22
AP
23

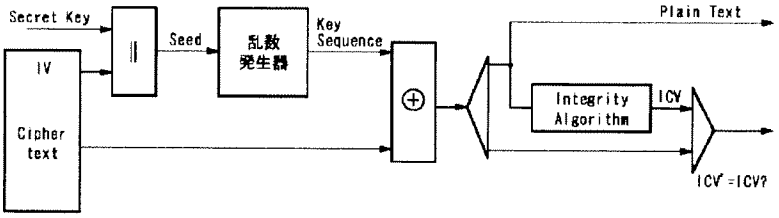
【図１０】


211
212
21
移動端末
無線LANカード
22
AP
24
保守サーバ
25
認証サーバ
23

【図７】

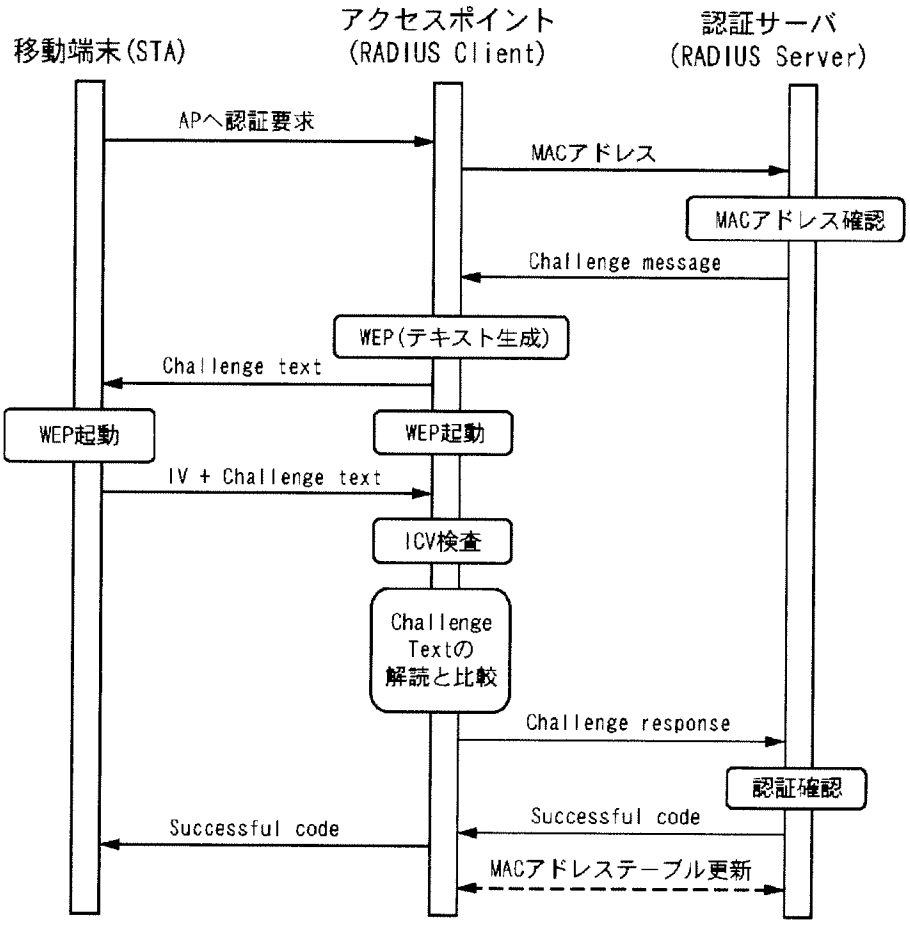

移動端末(STA)
アクセスポイント(AP)
P1
平文
Shared Key認証要求(MACアドレス)
Challenge Text
P2
Shared Key 認証
WEP起動 IV決定
WEP起動
P3
WEPで暗号化
Challenge Textのコピー + IV
ICV検査
Challenge Textの解読と比較
P4
認証成功

【図９】

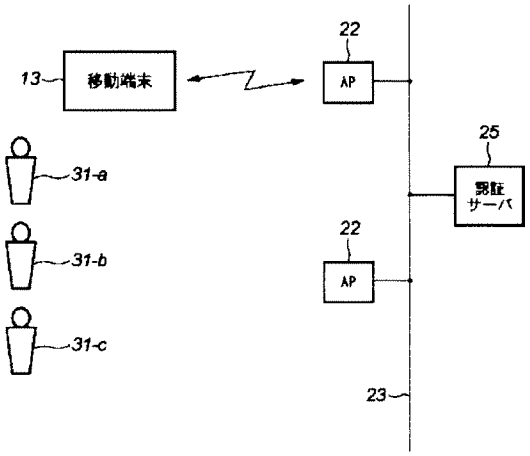


WEP暗号化ブロック

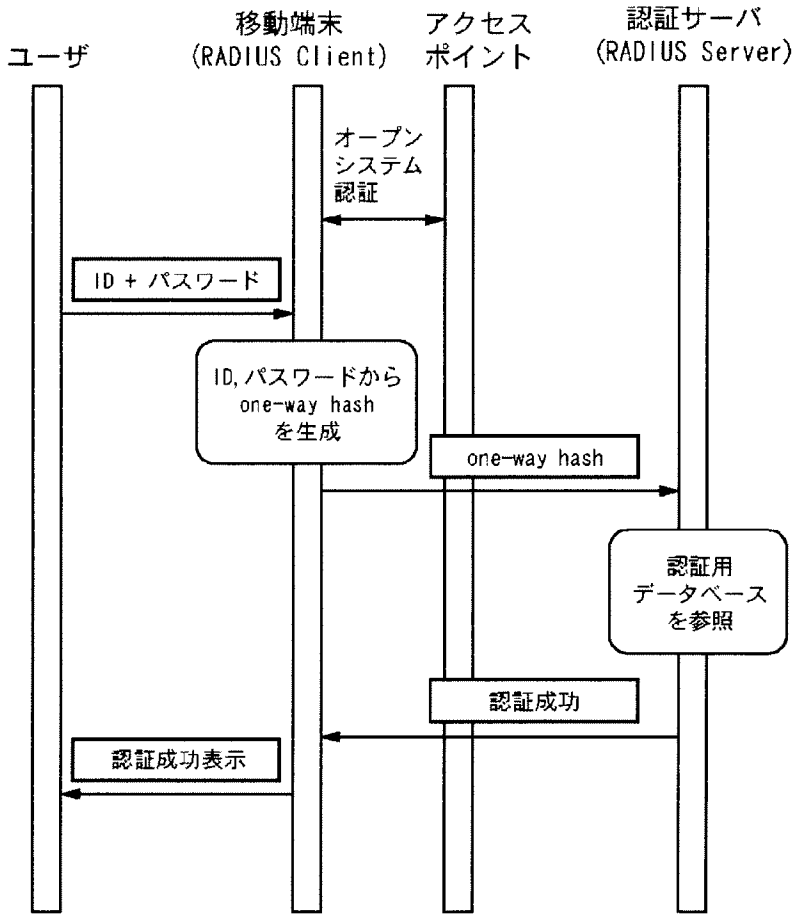
【図１１】



【図１２】


22
13
移動端末
AP
25
認証
サーバ
31-a
22
31-b
AP
31-c
23

【図１３】


ユーザ
移動端末
(RADIUS Client)
アクセス
ポイント
認証サーバ
(RADIUS Server)
オープン
システム
認証
ID + パスワード
ID,パスワードから
one-way hash
を生成
one-way hash
認証用
データベース
を参照
認証成功
認証成功表示

フロントページの続き

Ｆターム(参考) 5B035 AA13 AA14 BB09 BC00 CA29
5B058 CA02 KA01 KA02 KA04 KA06
KA12 KA31
5B085 AA08 AE03 AE04 AE12 AE23
AE29 BC01 BE01 BE04 BG02
BG07
5J104 AA07 AA16 EA01 EA04 EA22
JA01 JA03 KA01 KA04 MA01
NA02 NA05 NA12 NA33 NA38
NA41 PA01
5K067 AA32 DD17 EE02 EE10 FF02
FF23 HH21 HH23